

Bezpieczeństwo systemów komputerowych

Ogólne własności bezpieczeństwa informacji

Marcin Peczarski

Instytut Informatyki Uniwersytetu Warszawskiego

17 października 2011

Na podstawie materiałów Michała Szychowiaka
z <http://wazniak.mimuw.edu.pl>

Trzy podstawowe własności bezpieczeństwa informacji

- ▶ Confidentiality – poufność
- ▶ Integrity – integralność, nienaruszalność
- ▶ Availability – dostępność, dyspozycyjność

Inny zestaw własności bezpieczeństwa informacji

- ▶ Confidentiality – poufność
- ▶ Possesion – własność, posiadanie
- ▶ Integrity – integralność, nienaruszalność
- ▶ Authenticity – autentyczność, oryginalność
- ▶ Availability – dostępność, dyspozycyjność
- ▶ Utility – użyteczność, przydatność

Zagrożenia poufności informacji

- ▶ Nieuprawniony dostęp do danych w miejscu składowania, np. w bazie danych
- ▶ Nieuprawniony dostęp do danych w miejscu przetwarzania, np. w aplikacji końcowej użytkownika
- ▶ Podśluchanie danych przesyłanych w sieci
- ▶ Analiza fal elektromagnetycznych emitowanych przez urządzenia elektroniczne
- ▶ Analiza poboru prądu przez układy elektroniczne

Mechanizmy ochrony poufności informacji

- ▶ Uwierzytelnianie
- ▶ Autoryzacja i kontrola dostępu do zasobów
- ▶ Utrudnianie podsłuchu

Uwierzytelnianie

► Uwierzytelnianie jednokierunkowe:

- uwierzytelnianie jednego podmiotu (uwierzytelnianego), np. klienta aplikacji, wobec drugiego (uwierzytelniającego), np. serwera;
- weryfikacja danych uwierzytelniających przekazanych przez podmiot uwierzytelniany;
- typowe dane uwierzytelniające to identyfikator użytkownika i jego hasło dostępu.

► Uwierzytelnianie dwukierunkowe:

- kolejne lub jednoczesne uwierzytelnieniu obu podmiotów, które są wzajemnie i naprzemiennie uwierzytelnianym oraz uwierzytelniającym;
- jeżeli wzajemne uwierzytelnianie następuje sekwencyjnie (np. najpierw klient wobec serwera, a później serwer wobec klienta), mówimy o uwierzytelnianiu dwuetapowym;
- natomiast jednoczesne uwierzytelnienie obu stron nazywamy jednoetapowym.

Uwierzytelnianie, cd.

- ▶ **Uwierzytelnianie z udziałem zaufanej strony trzeciej:**
 - ▶ w procesie uwierzytelniania uczestniczy zaufana strona trzecia;
 - ▶ strona trzecia bierze na siebie ciężar weryfikacji danych uwierzytelniających podmiotu uwierzytelnianego;
 - ▶ po pomyślnej weryfikacji podmiot uwierzytelniany otrzymuje poświadczenie, które następnie przedstawia zarządcy zasobu (serwerowi), do którego dostępu żąda;
 - ▶ podstawową zaletą tego podejścia jest przesunięcie newralgicznej operacji uwierzytelniania do wyróżnionego stanowiska, które można poddać szczególnie podwyższonemu zabezpieczeniu;
 - ▶ należy też podkreślić potencjalną możliwość wielokrotnego wykorzystania wydanego poświadczenia (przy dostępie klienta do wielu zasobów, serwerów);
 - ▶ zaufana strona trzecia może być lokalna dla danej sieci komputerowej (korporacyjnej) lub zewnętrzna (wykorzystująca infrastrukturę uwierzytelniania dostępną w sieci rozległej, np. publiczne urzędy certyfikujące).

Uwierzytelnianie za pomocą identyfikatora i hasła

- ▶ Jest to klasyczny i najpowszechniejszy sposób uwierzytelniania.
- ▶ Serwer żąda od klienta podania identyfikatora (ang. *login*) i hasła (ang. *password*).
- ▶ Wiele protokołów sieciowych i aplikacji, zwłaszcza zaprojektowanych dawniej, przesyła dane uwierzytelniające jawnym tekstem.
- ▶ Stosowanie tej metody wymaga jednoczesnej ochrony przed podsłuchaniem.

Słabości uwierzytelniania za pomocą hasła

- ▶ Hasło można złamać metodą przeszukiwania wyczerpującego (ang. *brute-force attack*).
- ▶ Hasło można odgadnąć, używając ataku słownikowego (ang. *dictionary attack*).
- ▶ Hasło można podsłuchać w trakcie niezabezpieczonej transmisji.
- ▶ Hasło można wykraść z systemowej bazy haseł użytkowników:
 - ▶ zwykle hasła nie są przechowywane w postaci jawnej,
 - ▶ często są zakodowane funkcją jednokierunkową lub zaszyfrowane,
 - ▶ jednak niekiedy można stosunkowo łatwo je pobrać i następnie starać się odzyskać ich oryginalną postać.
- ▶ Hasło można pozyskać inną metodą, np. kupić.

Słabości uwierzytelniania za pomocą hasła

- ▶ Hasła się starzeją:
 - ▶ czas, przez który możemy z dużą pewnością polegać na tajności hasła, skraca się nieustannie;
 - ▶ hasła wymagają systematycznych zmian.
- ▶ W niektórych środowiskach aplikacyjnych stosuje się predefiniowane konta użytkowników:
 - ▶ również o charakterze administracyjnym;
 - ▶ zwykle przypisuje się im dość powszechnie znane hasła domyślne;
 - ▶ usuwanie lub dezaktywowanie takich kont czy zmiana haseł wymagają dużej staranności.

Atak słownikowy

- ▶ Zgromadź nazwy użytkowników, ich inicjały oraz inne dostępne informacje, np. daty urodzin.
- ▶ Dodaj imiona, nazwy miejsc, nazwiska sławnych ludzi, tytuły filmów i książek s.f. oraz nazwiska sportowców i terminy sportowe.
- ▶ Dodaj słowa z lokalnego słownika korekty językowej.
- ▶ Utwórz permutacje słów ze słownika.
- ▶ Zmień pierwszą literę na wielką.
- ▶ Zastąp pierwszą literę znakiem sterującym.
- ▶ Zmień litery o na 0 czy l na 1.
- ▶ Utwórz liczbę mnogą.
- ▶ Dodawaj przed- i przyrostki.
- ▶ Próbuj kombinacji małych i wielkich liter.

Przeszukiwanie wyczerpujące

- ▶ Przeszukiwanie wyczerpujące (atak brutalny) polega na sprawdzeniu całej przestrzeni haseł, czyli wybieraniu wszystkich możliwych permutacji znaków z alfabetu wykorzystywanego przy ustawianiu hasła użytkownika.
- ▶ Maksymalny czas używania hasła wyraża wzór

$$L \leq \frac{S}{R},$$

gdzie L to czas obowiązywania hasła, R to ilość możliwych do wykonania prób złamania hasła na jednostkę czasu, a S to rozmiar przestrzeni haseł.

- ▶ W praktyce czas ten powinien być dużo krótszy.

Żelazne reguły higieny haseł

► Nie wolno:

- wybierać hasła o długości krótszej niż 8 znaków;
- wybierać jako hasła powszechnego słowa, imienia, nazwiska, daty urodzenia, numeru telefonu, numeru rejestracyjnego;
- zmieniać hasła tak, aby nowe było zależne od starego (np. z 012345 na 123456 albo z Xyz01 na Xyz02);
- używać tego samego hasła w więcej niż jednym miejscu;
- zapisywać hasła w widocznych lub łatwo dostępnych miejscach, jak np. fragment biurka zakryty klawiaturą, wewnątrz szuflady czy płyta z danymi;
- informować nikogo o swoim hasle.

► Należy:

- wybierać długie i mało znane słowo lub frazę (kombinacja różnych znaków);
- wybrać hasło w sposób na tyle losowy na ile to tylko możliwe;
- zmieniać hasło możliwie często, lecz w nieprzewidywalny sposób;
- zmienić hasło natychmiast, jak tylko rodzi się podejrzenie, że ktoś mógł je poznać.

Żelazne reguły higieny haseł, cd.

- ▶ Warto:
 - ▶ opracować własny algorytm generowania haseł – wybór pierwszych liter słów ulubionej fraszki, ostatnich znaków z wersów wiersza lub wybranej strony książki itp.;
 - ▶ zlecić systemowi wygenerowanie trudnego hasła.

Zdalne potwierdzanie tożsamości użytkownika

- ▶ Np. oparte o usługę *ident* opisaną w RFC 1413.
- ▶ Użytkownik uruchamia klienta usługi xyz i nawiązuje połączenie z serwerem xyz.
- ▶ Serwer xyz, w celu poświadczenia nazwy (lub identyfikatora) użytkownika wykorzystującego usługę, kontaktuje się z serwerem *ident* nasłuchującym na stacji klienta na porcie 113 TCP.
- ▶ W standardzie RFC 1413 oraz w praktycznych implementacjach nie realizuje się uwierzytelniania podmiotu żądającego informacji z tej usługi.
- ▶ Należy zdawać sobie sprawę z potencjalnych zagrożeń, jakie niesie udostępnianie przez usługę *ident* informacji o przynależności procesów dokonujących komunikacji sieciowej (nie tylko klientów).
- ▶ Może ona być zatem również nadużyta przez potencjalnego włamywacza.

Uwierzytelnianie jednokrotne (ang. *single sign-on*)

- ▶ Minimalizacja ilości wystąpień danych uwierzytelniających – hasło powinno być podawane jak najrzadziej.
- ▶ Jeśli jeden z komponentów systemu (np. system operacyjny) dokonał pomyślnie uwierzytelnienia użytkownika, pozostałe komponenty (np. inne systemy lub zarządcy zasobów) będą ufać tej operacji i nie będą samodzielnie wymagać podawania ponownie danych uwierzytelniających.
- ▶ Teoretycznie jest możliwe, że każdy komponent korzysta z własnego mechanizmu uwierzytelniania.
- ▶ Wówczas, dodatkowo po pierwszorazowym uwierzytelnieniu użytkownika, system może oddelegować specjalny moduł do przechowywania odrębnych danych uwierzytelniających użytkownika i poświadczania w przyszłości jego tożsamości wobec innych komponentów systemu.

Hasło jednorazowe (ang. *one-time password*)

- ▶ Konkretna postać hasła użyta zostaje tylko raz.
- ▶ Hasło staje się bezwartościowe po przechwyceniu.
- ▶ Sposoby generowania haseł jednorazowych:
 - ▶ lista haseł,
 - ▶ synchronizacja czasu,
 - ▶ metoda zwołanie-odzew.
- ▶ Dostępne postacie haseł jednorazowych:
 - ▶ listy papierowe,
 - ▶ listy zdrapki,
 - ▶ znaczniki (ang. *token*) programowe,
 - ▶ znaczniki sprzętowe.

Listy haseł jednorazowych

- ▶ Jest to najprostsza i najtańsza metoda zastosowania haseł jednorazowych.
- ▶ Użytkownik otrzymuje listę zawierającą ponumerowane hasła.
- ▶ Ta sama lista jest zapisana w bazie systemu identyfikującego.
- ▶ W trakcie logowania użytkownik podaje swój identyfikator, a system prosi o podanie hasła z odpowiednim numerem.
- ▶ Klient za każdym razem posługuje się kolejnym niewykorzystanym hasłem z listy.

Metoda z synchronizacją czasu (ang. *time synchronization*)

- ▶ Klient generuje unikalny kod w funkcji pewnych parametrów użytkownika (identyfikator, kod pin, hasło, numer seryjny karty identyfikacyjnej) oraz bieżącego czasu.
- ▶ Serwer weryfikuje otrzymany od klienta kod, korzystając z identycznej funkcji (z odpowiednią tolerancją czasu).

Metoda zwołanie-odzew (ang. *challenge-response*)

- ▶ Serwer pyta o nazwę użytkownika, a następnie przesyła unikalny ciąg (zwołanie).
- ▶ Klient koduje otrzymany ciąg (np. swoim hasłem lub innym tajnym parametrem pełniącym rolę klucza) i odsyła jako odzew.
- ▶ Serwer, posługując się identycznym kluczem, weryfikuje poprawność odzewu.

Znaczniki

- ▶ Znacznik (ang. *token*) programowy to specjalny program, który w zależności od implementacji generuje hasło jednorazowe na podstawie czasu lub zawołania serwera.
- ▶ Znacznik sprzętowy jest małym przenośnym urządzeniem spełniającym wszystkie funkcje znacznika programowego.
- ▶ Popularne jest wykorzystywanie telefonu komórkowego (np. przez operatorów telefonii komórkowej) do uwierzytelniania za pomocą haseł jednorazowych:
 - ▶ hasło jednorazowe przesyłane jest z serwera na telefon w postaci SMS;
 - ▶ rola telefonu sprowadza się tylko do medium odbierającego i wyświetlającego dane;
 - ▶ bezpieczeństwo tej metody jest wątpliwe.

Inne mechanizmy uwierzytelniania

- ▶ Uwierzytelniany użytkownik musi wykazać się posiadaniem odpowiedniego przedmiotu:
 - ▶ karta magnetyczna,
 - ▶ karta mikroprocesorowa,
 - ▶ klucz, znacznik (ang. *token*) USB.
- ▶ W przypadku ludzi można posłużyć się cechami biometrycznymi:
 - ▶ odcisk palca,
 - ▶ geometria twarzy,
 - ▶ tęcza oka,
 - ▶ obraz siatkówki,
 - ▶ odcisk dłoni,
 - ▶ obraz żył krwionośnych,
 - ▶ podpis odręczny,
 - ▶ głos,
 - ▶ DNA.

Autoryzacja i kontrola dostępu do zasobów

- ▶ Autoryzacja i kontrola dostępu użytkowników należy do podstawowych funkcji systemu operacyjnego, systemu zarządzania bazą danych lub środowiska przetwarzania rozproszonego.
- ▶ Aktualnie jednym z najczęściej stosowanych mechanizmów weryfikacji praw dostępu jest lista kontroli dostępu.
- ▶ Implementacja listy kontroli dostępu, w zależności od konkretnego systemu, nazywa się ACL (ang. *Access Control List*), ARL (ang. *Access Rights List*) lub Trustees.
- ▶ Ogólna koncepcja działania mechanizmu listy kontroli polega na wyspecyfikowaniu dla każdego udostępnianego zasobu listy indywidualnych użytkowników lub ich grup, bądź kategorii oraz przydzieleniu im podzbiorów uprawnień wybranych ze zbioru wszystkich uprawnień dostępnych dla danego zasobu.

Utrudnianie podsłuchu

- ▶ Podsłuch jest zwykle skierowany przeciwko określonym zasobom i ma konkretny cel, np. przechwycenie hasła lub zawartości konkretnych plików.
- ▶ Atak taki w istocie polega na wykonaniu operacji umożliwiających dostęp do kanału transmisyjnego (wpięcie się do medium transmisyjnego, podłączenie do stacji bazowej sieci bezprzewodowej itp.), a następnie na wyłuskaniu poszukiwanych informacji z całego ruchu odbywającego się w tym kanale.
- ▶ Ogólna koncepcja utrudniania podsłuchu polega zatem na uczynieniu możliwie jak najbardziej kłopotliwym obu kroków ataku – wpięcia się do kanału komunikacyjnego i wyłuskania użytecznych danych.

Utrudnianie podsłuchu, cd.

- ▶ Należy stosować topologię sieciową utrudniającą ewentualny podsłuch lub ułatwiającą jego wykrycie, np. topologię gwiazdy zamiast topologii liniowej czy pierścieniowej.
- ▶ Stosowanie medium mniej podatnego na podsłuch:
 - ▶ światłowód jest mniej podatny na podsłuch niż kabel elektryczny,
 - ▶ kable ekranowane są mniej podatne na podsłuch niż kable nieekranowane,
 - ▶ sieć kablowa jest mniej podatna na podsłuch niż sieć bezprzewodowa.

Utrudnianie podsłuchu przez ograniczanie emisji elektromagnetycznej

- ▶ Przechwytywanie promieniowania elektromagnetycznego emitowanego przez układy komputera jest nadal tańsze od innych typów ataków na poufność danych (np. ataku kryptoanalitycznego), mimo że wymaga bardzo specjalistycznego sprzętu.
- ▶ Taki atak można skutecznie utrudnić, wykorzystując materiały pochłaniające promieniowanie elektromagnetyczne.
- ▶ Należy ekranować obudowy komputerów i urządzeń peryferyjnych oraz pomieszczenia (specjalne szyby, tapety, wykładziny podłogowe i sufitowe).

Utrudnianie podsłuchu przez ograniczanie emisji elektromagnetycznej, cd.

- ▶ W niektórych zastosowaniach, jak np. przetwarzanie danych niejawnych, obowiązuje standard TEMPEST (ang. *Transient Electromagnetic Pulse Emanation Standard*), który definiuje wymagania stanowiska komputerowego o ograniczonej emisji elektromagnetycznej.
- ▶ Stanowisko komputerowe zgodne z TEMPEST to wydatek rzędu kilkunastu, kilkudziesięciu tysięcy złotych.

Inne metody utrudniania podsłuchu

- ▶ Utrudnianie wyłuskania użytecznych danych przez sztuczne generowanie ruchu (ang. *traffic padding*):
 - ▶ wypełnianie wolnego pasma przenoszenia sieci bezużytecznymi danymi;
 - ▶ w wyniku zwiększenia proporcji danych bezużytecznych w całym ruchu rozróżnienie danych użytecznych od reszty jest potencjalnie trudniejsze.
- ▶ Tworzenie zamkniętych grup użytkowników przez separację ruchu sieciowego, wspierane przez technologie sieci wirtualnych VLAN ACL, Wire-rate ACL i in.
- ▶ Kontrola dostępu do zasobów infrastruktury sieciowej przez dopuszczanie do udziału w ruchu sieciowym tylko uwierzytelnionych stacji sieciowych, co realizuje np. protokół IEEE 802.1X.
- ▶ **Szyfrowanie** danych stanowi niewątpliwie najbardziej uniwersalny mechanizm ochrony poufności danych i – jak zobaczymy wkrótce – szerzej rozumianej ochrony danych. Będą mu poświęcone kolejne wykłady.

Zagrożenia integralności informacji

- ▶ Nieautoryzowana modyfikacja (dostęp do zapisu, w odróżnieniu od poufności, która oznacza ochronę przed nieautoryzowanym dostępem do odczytu)
- ▶ Celowa lub przypadkowa modyfikacja danych przez nieuprawnionych użytkowników bądź oprogramowanie (np. wirusowe)

Mechanizmy ochrony integralności informacji

- ▶ Wymienione wcześniej mechanizmy kontroli dostępu do danych
- ▶ Suma kontrolna zbioru danych (np. pliku dyskowego)
- ▶ Kryptograficzna suma kontrolna i podpis elektroniczny
- ▶ Rejestracja operacji na danych (ang. *audit*) – niezbędna dla formalnego wykrycia naruszeń integralności; zwykle spotyka się podział danych audytu co najmniej na
 - ▶ dziennik zdarzeń systemowych,
 - ▶ dziennik zdarzeń aplikacji.
- ▶ Kontrola antywirusowa

Zagrożenia dostępności informacji

▶ Przyczyny

- ▶ uszkodzenie sprzętu
- ▶ awaria łącza komunikacyjnego
- ▶ awaria zasilania
- ▶ awaria klimatyzacji
- ▶ konieczność wykonania uaktualnienia oprogramowania
- ▶ atak typu odmowa usługi (ang. *DoS*)
- ▶ efekt wtórny innego typu ataku

▶ Skutki

- ▶ utrata przez uprawnione osoby możliwości korzystania z systemu
- ▶ utrata dostępu do zasobów
- ▶ przerwa w działaniu serwisu
- ▶ niedostępność usługi

Mechanizmy ochrony dostępności informacji

- ▶ Działania zapobiegawcze
- ▶ Środki automatyczne:
 - ▶ rozwiązania programowe,
 - ▶ rozwiązania sprzętowe.
- ▶ Likwidacja skutków utraty dostępności:
 - ▶ kopie zapasowe,
 - ▶ przełączenie na rezerwowe składniki systemu.