

Bezpieczeństwo systemów komputerowych

Wprowadzenie

Marcin Peczarski

Instytut Informatyki Uniwersytetu Warszawskiego

2 października 2011

O przedmiocie

- ▶ Wykład

<http://www.mimuw.edu.pl/~marpe/bsk>

- ▶ Laboratorium

<http://smurf.mimuw.edu.pl/drupal6/node/84>

- ▶ Zaliczenie:

- ▶ do zdobycia są po 24 punkty z laboratorium i z egzaminu,
- ▶ o ocenie końcowej zadecyduje suma punktów.

Źródła

- ▶ Michał Szychowiak: *Bezpieczeństwo systemów komputerowych*, <http://wazniak.mimuw.edu.pl>.
- ▶ William Stallings: *Ochrona danych w sieci i intersieci. W teorii i praktyce*, WNT, Warszawa 1997.
- ▶ Michael Howard, David LeBlanc: *Bezpieczny kod. Tworzenie i zastosowanie*, Microsoft Press, Warszawa 2002.
- ▶ Bruce Schneier: *Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C*, WNT, Warszawa 1995, 2002.
- ▶ Janusz Stokłosa, Tomasz Bilski, Tadeusz Pankowski: *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Warszawa–Poznań 2001.

Co to jest bezpieczeństwo?

- ▶ System komputerowy jest **bezpieczny**, jeśli:
 - ▶ jego użytkownik może na nim polegać,
 - ▶ oprogramowanie działa zgodnie ze swoją specyfikacją,
- ▶ a wprowadzone dane:
 - ▶ nie zostaną utracone,
 - ▶ nie ulegną zniekształceniu,
 - ▶ nie zostaną pozyskane przez kogoś nieuprawnionego.

System bezpieczny a wiarygodny

- ▶ Bezpieczeństwo jest elementem szerszego kontekstu, nazywanego wiarygodnością systemu komputerowego.
- ▶ System komputerowy jest **wiarygodny**, jeśli jest:
 - ▶ **dyspozycyjny** (ang. *available*) – dostępny na bieżąco,
 - ▶ **niezawodny** (ang. *reliable*) – odporny na awarie,
 - ▶ **bezpieczny** (ang. *secure*) – zapewniający ochronę danych,
 - ▶ **bezpieczny** (ang. *safe*) – bezpieczny dla otoczenia.
- ▶ Proszę zwrócić uwagę na dwa angielskie terminy **secure** i **safe** odpowiadające polskiemu przymiotnikowi **bezpieczny**.

Znaczenie bezpieczeństwa

- ▶ Techniki komputerowe (bądź szerzej mikroprocesorowe) są wszechobecne.
- ▶ Trudno konstruuje się systemy bezpieczne:
 - ▶ technologie są niedoskonałe,
 - ▶ ludzie są omylni,
 - ▶ zapewnienie bezpieczeństwa wymaga poświęcenia dodatkowego czasu na projektowanie i testowanie;
 - ▶ obecność konkurencji powoduje presję wprowadzania nowych, niedostatecznie bezpiecznych produktów.
- ▶ System musi być jeszcze właściwie eksploatowany:
 - ▶ konfigurowanie uprawnień dostępu do zasobów,
 - ▶ stosowanie silnych haseł.
- ▶ Występuje konflikt interesów między użytecznością technologii a ryzykiem niewłaściwego jej wykorzystania:
 - ▶ telefonu komórkowego można użyć do zdetonowania bomby,
 - ▶ odpluskwiacz (ang. *debugger*) może pomóc złamać zabezpieczenia programu komputerowego.

Zagrożenia bezpieczeństwa

- ▶ Natura zagrożeń:
 - ▶ przypadkowe (nieświadość lub naiwność użytkownika),
 - ▶ efekt celowego działania (chęć zysku, poklasku lub odwetu),
 - ▶ pochodzące z zewnątrz organizacji,
 - ▶ pochodzące od środka organizacji.
- ▶ Przestępstwa komputerowe:
 - ▶ włamanie do systemu komputerowego,
 - ▶ nieuprawnione pozyskanie informacji,
 - ▶ destrukcja danych i programów,
 - ▶ sabotaż (sparaliżowanie pracy) systemu,
 - ▶ piractwo komputerowe, kradzież oprogramowania,
 - ▶ oszustwo komputerowe i fałszerstwo komputerowe,
 - ▶ szpiegostwo komputerowe.

Fragmenty kodeksu karnego

Art. 267. §1. Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§2. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym.

§3. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1 lub 2 ujawnia innej osobie.

§4. Ściganie przestępstwa określonego w § 1–3 następuje na wniosek pokrzywdzonego.

Fragmenty kodeksu karnego

Art. 268. §1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§2. Jeżeli czyn określony w § 1 dotyczy zapisu na komputerowym nośniku informacji, sprawca podlega karze pozbawienia wolności do lat 3.

§3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§4. Ściganie przestępstwa określonego w § 1–3 następuje na wniosek pokrzywdzonego.

Fragmenty kodeksu karnego

Art. 269. §1. Kto, na komputerowym nośniku informacji, niszczy, uszkadza, usuwa lub zmienia zapis o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub administracji samorządowej albo zakłóca lub uniemożliwia automatyczne gromadzenie lub przekazywanie takich informacji, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając nośnik informacji lub niszcząc albo uszkadzając urządzenie służące automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji.

Fragmenty kodeksu karnego

Art. 287. §1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji lub zmienia, usuwa albo wprowadza nowy zapis na komputerowym nośniku informacji, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

§3. Jeżeli oszustwo popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

Przed kim się bronimy?

- ▶ **Haker** (ang. *hacker*) – **zapalony komputerowiec**:
 - ▶ osoba, której przyjemność sprawia poznawanie szczegółów działania systemów komputerowych i rozszerzanie swych umiejętności w tym zakresie, w przeciwieństwie do większości użytkowników chcących poznać tylko niezbędne minimum wiedzy potrzebnej do obsługi komputera;
 - ▶ osoba, która entuzjastycznie zajmuje się programowaniem i nie lubi teorii dotyczącej tej dziedziny;
 - ▶ powszechne, choć niezupełnie słuszne, określenie osoby podejmującej atak na system komputerowy.
- ▶ **Agresor**:
 - ▶ osoba podejmująca atak na system komputerowy;
 - ▶ kraker (ang. *cracker*), intruz, włamywacz, napastnik, wandal, przestępca.

Co powinno być chronione?

- ▶ Stanowiska komputerowe
- ▶ Infrastruktura sieciowa
- ▶ System operacyjny
- ▶ Usługi narzędziowe
- ▶ Aplikacje użytkowe

Poziom bezpieczeństwa

- ▶ Nie istnieje system **absolutnie bezpieczny**:
 - ▶ nie możemy przewidzieć wszystkich możliwych zagrożeń;
 - ▶ szybki rozwój technologii implikuje powstawanie coraz to nowych zagrożeń;
 - ▶ czas reakcji na nowe zagrożenia nie jest zerowy;
 - ▶ ludzka niedoskonałość, w szczególności omylność projektantów, programistów, użytkowników systemów informatycznych, skutkuje błędami w oprogramowaniu oraz niewłaściwym lub niefrasobliwym jego wykorzystaniem.
- ▶ System jest **dostatecznie bezpieczny**, jeśli agresor rezygnuje z ataku, gdyż:
 - ▶ sforsowanie zabezpieczeń jest zbyt czasochłonne;
 - ▶ atak jest nieopłacalny, poniesione nakłady przekraczają ewentualne zyski.
- ▶ Nie można udowodnić, że system jest bezpieczny.
- ▶ Można tylko wykazać, pokazując metodę ataku, słabości w bezpieczeństwie.

Strategie ataku

- ▶ Agresor na ogół nie pokonuje zabezpieczeń, tylko je obchodzi.
- ▶ Skuteczny atak na aktywny mechanizm zabezpieczeń jest raczej czasochłonny i stosowany tylko w ostateczności.
- ▶ Zwykle mniej kosztowne i szybsze jest znalezienie luki w oprogramowaniu i wtargnięcie do systemu „z boku”.
- ▶ Większość ataków przeprowadzana jest „od środka organizacji”, czyli przez zaufanych użytkowników, którzy łatwiej mogą znaleźć i wykorzystać luki w bezpieczeństwie.
- ▶ Agresor może wykorzystać:
 - ▶ chwilową nieobecność użytkownika;
 - ▶ boczne wejście do systemu, stworzone w celu „ułatwienia” jego pielęgnacji;
 - ▶ publicznie dostępne informacje o używanym oprogramowaniu;
 - ▶ podstęp, udawanie pracownika serwisu, dostawcy;
 - ▶ wymuszenie, szantaż;
 - ▶ przeszukanie śmieci, wyrzucanej makulatury lub nośników danych.

Linie obrony

- ▶ Możliwe jest obejście każdego mechanizmu zabezpieczeń.
- ▶ Zabezpieczenia powinny być konstruowane wielopoziomowo:
 - ▶ złamanie jednej linii obrony nie powinno umożliwiać wtargnięcia do systemu;
 - ▶ np. ochrona sieci ścianą ogniową (ang. *firewall*) nie zwalnia od tworzenia aplikacji odpornych na ataki z sieci zewnętrznej.
- ▶ Przejrzysta i modułarna konstrukcja systemu ułatwia ochronę.
- ▶ Wzrost poziomu bezpieczeństwa odbywa się kosztem wygody użytkowników.
- ▶ Brak symptomów ataku nie oznacza, że system nie został zaatakowany.
- ▶ Zaobserwowanie ataku nie jest trywialne nawet w systemie poprawnie monitorowanym.
- ▶ Symptomy ataku zwykle występują dopiero po jego zakończeniu, kiedy to może być zbyt późno, aby przeprowadzić akcję ratunkową, kiedy ucierpiały już newralgiczne składniki systemu, poufne dane lub reputacja firmy.

Strategia bezpieczeństwa

- ▶ O bezpieczeństwie należy myśleć już od początku etapu projektowania systemu informatycznego lub aplikacji.
- ▶ Błędy lub zaniedbania popełnione na etapie projektowania są trudne do naprawienia w późniejszych fazach projektu.
- ▶ Należy udzielić odpowiedzi na pytania:
 - ▶ Co chronić (określenie zasobów)?
 - ▶ Przed czym chronić (identyfikacja zagrożeń)?
 - ▶ Ile czasu, wysiłku i pieniędzy można poświęcić na ochronę (oszacowanie ryzyka, analiza kosztów i zysku)?

Przykłady chronionych zasobów

- ▶ Sprzęt komputerowy
- ▶ Infrastruktura sieciowa
- ▶ Wydruki
- ▶ Strategiczne dane
- ▶ Kopie zapasowe
- ▶ Wersje instalacyjne oprogramowania
- ▶ Dane osobowe
- ▶ Dane audytu
- ▶ Zdrowie pracowników
- ▶ Prywatność pracowników
- ▶ Zdolności produkcyjne
- ▶ Wizerunek publiczny i reputacja

Przykładowe zagrożenia

- ▶ Włamywacze komputerowi
- ▶ Infekcje wirusami
- ▶ Nieuczciwi pracownicy lub personel zewnętrzny
- ▶ Błędy w programach
- ▶ Kradzież nośników danych, komputerów (również w podróży służbowej)
- ▶ Utrata możliwości korzystania z łączy telekomunikacyjnych
- ▶ Bankructwo firmy serwisowej lub producenta sprzętu
- ▶ Choroba administratora lub kierownika projektu (jednoczesna choroba wielu osób)
- ▶ Powódź

Polityka bezpieczeństwa

- ▶ Powinna być elementem polityki biznesowej firmy.
- ▶ Etapy realizacji:
 - ▶ zaprojektowanie,
 - ▶ zaimplementowanie,
 - ▶ zarządzanie (w tym monitorowanie i okresowe audyty bezpieczeństwa).
- ▶ Zakres tematyczny:
 - ▶ definicja celu i misji polityki bezpieczeństwa,
 - ▶ standardy i wytyczne których przestrzegania wymagamy,
 - ▶ kluczowe zadania do wykonania,
 - ▶ zakresy odpowiedzialności.
- ▶ Specyfikacja środków:
 - ▶ ochrona fizyczna,
 - ▶ polityka proceduralno-kadrowa (odpowiedzialność personalna),
 - ▶ rozwiązania techniczne, informatyczne.

Normy i zalecenia zarządzania bezpieczeństwem

- ▶ Stworzono wiele dokumentów poświęconych realizacji polityki bezpieczeństwa.
- ▶ Norma ISO/IEC Technical Report 13335 (ratyfikowana w naszym kraju jako PN-I-13335) obejmuje:
 - ▶ TR 13335-1 – terminologia i modele;
 - ▶ TR 13335-2 – metodyka planowania i prowadzenia analizy ryzyka, specyfikacja wymagań stanowisk pracy związanych z bezpieczeństwem systemów informatycznych;
 - ▶ TR 13335-3 – techniki zarządzania bezpieczeństwem:
 - ▶ zarządzanie ochroną informacji,
 - ▶ zarządzanie konfiguracją systemów IT,
 - ▶ zarządzanie zmianami;
 - ▶ TR 13335-4 – metodyka doboru zabezpieczeń;
 - ▶ WD 13335-5 – zabezpieczanie połączeń z sieciami zewnętrznymi.
- ▶ Należałoby wymienić tu jeszcze kilkadziesiąt norm.
- ▶ Nikt nie jest w stanie tego wszystkiego przeczytać w rozsądnym czasie.