Przedstawienie możliwych zagrożeń przy tworzeniu aplikacji

Temat I

Możliwe ataki na oprogramowanie

- Wirusy
- Internetowe robaki
- Podmiana zawartości strony WWW
- Przewidzenie działania serwisu (poker)
- (Częściowe) Przejęcie sterowania systemem

Zwiększenie narażenia na ataki

- Bardziej skomplikowane oprogramowanie
- Oprogramowanie narażone na ciągłe ataki (sieć)

Typowe środki zapobiegawcze

- Regularne uaktualnianie oprogramowania
- Instalowanie ścian ogniowych
- Pasywne i aktywne monitorowanie sieci

Bezpieczeństwo oprogramowania

- Bezpieczeństwo = sterowanie dostępem do cennych rzeczy

- Oprogramowanie oferuje *funkcjonalność*
- Niektóre funkcjonalności związane są z *ryzykiem*
- Bezpieczeństwo oprogramowania = *zarządzanie tym ryzykiem*

Bezpieczeństwo a funkcjonalność

- Funkcjonalność to *podstawowy* cel tworzenia oprogramowania
- Bezpieczeństwo to *dodatkowy* cel przy tworzeniu oprogramowania
- Często funkcjonalność stoi w konflikcie z bezpieczeństwem

komputer odłączony od sieci nie jest narażony na ataki z sieci

Typowe wymagania bezpieczeństwa

- CIA: confidentiality, integrity, availability
- non-repudiation (niemożność wyparcia się)
- authentification
- access control

Hierarchia ważności wymagań

1. Integralność – transakcje bankowe, zapisy medyczne
2. Niemożność wyparcia się – decyzje (przelanie pieniędzy)
3. Tajność – konkurencja nie powinna wiedzieć
4. Autentyczność – dostęp powinna mieć tylko osoba upoważniona
5. Kontrola dostępu – zakres dostępności powinien być przestrzegany
6. Dostępność – brak dostępu do konta bankowego denerwuje

Jak spełnić wymagania bezpieczeństwa?

- Prewencja – zabezpieczanie się przed zniszczeniem wartości (ściany ogniowe, zmienianie haseł, okresowe uaktualnianie oprogramowania),
- Wykrywanie – wykrywanie możliwości i przypadków zniszczenia wartości (monitorowanie systemu i sieci, szukanie błędów w oprogramowaniu),
- Reakcja – odnawianie zniszczonych wartości oraz wykrywanie i karanie sprawców (ustawianie nowego hasła, uaktualnianie oprogramowania po włamaniu, zawiadomienie organów).

Typowe zagrożenia dla wymagań

- Tajność – wyciek informacji
- Integralność – podmiana informacji, zniszczenie treści
- Dostępność – ataki denial-of-service
- Autentyczność – podszycie się
- Kontrola dostępu – naruszenie zasad dostępu

Zabezpieczenia

- Mogą być fizyczne i społeczne
  - grube ściany,
  - przeszukiwanie pracowników,
  - procedury wygasania haseł,
  - procedury sądowo-policyjne.
- nie będziemy się tym tutaj zajmować...

Zabezpieczenia i nowe zagrożenia

- Zabezpieczenia mogą prowadzić do nowych zagrożeń
  - Wprowadzamy możliwość 3 loginów, aby zapobiec atakom siłowym
  - Jakie nowe zagrożenia powstają?

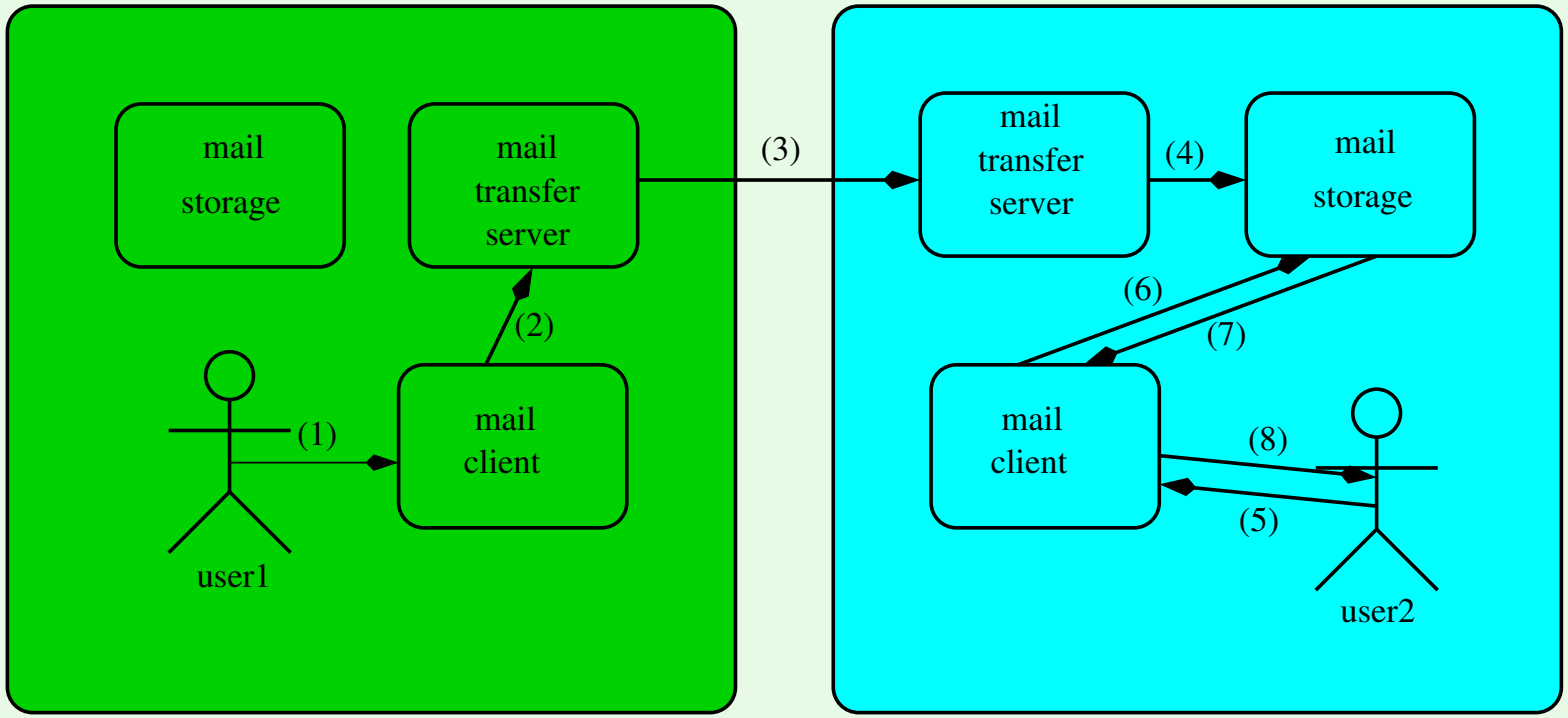
- Łatanie dziur w oprogramowaniu wprowadza nowe pluskwy
  - SSH wprowadzono, aby umożliwić bezpieczną pracę, ale...

Zabezpieczenia i nowe zagrożenia

- Zabezpieczenia mogą prowadzić do nowych zagrożeń
  - Wprowadzamy możliwość 3 loginów, aby zapobiec atakom siłowym
  - Jakie nowe zagrożenia powstają?

- Łatanie dziur w oprogramowaniu wprowadza nowe pluskwy
  - SSH wprowadzono, aby umożliwić bezpieczną pracę, ale
  - implementacje SSH zawierają błędy, które narażają serwery

System pocztowy



Potencjalne zagrożenia systemu pocztowego

- Podpatrzenie e-maila
  - dane przesyłane przez Internet łatwo podpatrzeć
  - zatem treść e-maili nie jest w najmniejszym stopniu tajna
- Modyfikacja e-maila
  - przejęcie komunikacji (np. między dwoma serwerami pocztowymi) pozwala atakującemu na zmodyfikowanie e-maila
  - zatem integralność e-maili nie może być zagwarantowana

Potencjalne zagrożenia systemu pocztowego

- Podszywanie się
  - serwery pocztowe ślepo wierzą w informacje o nadawcy
  - zatem nie ma gwarancji co do autentyczności nadawcy
- Ataki na serwery pocztowe
  - serwer pocztowy jest „zaufaną warstwą” oferującą ograniczony dostęp do systemu
  - jeśli można włamać się do programu i przekroczyć te ograniczenia, to można zaatakować maszynę serwera

Potencjalne zagrożenia systemu pocztowego

- Spam
  - marketingowiec może wysyłać duże ilości niepożądanych wiadomości
- Ataki denial-of-service
  - np. wolne miejsce na serwerze dyskowym poczty może zostać zajęte przez bardzo duże e-maile
- Ataki na klienty pocztowe
  - klient pocztowy jest „zaufaną warstwą” oprogramowania,
  - możliwość wykonywania programów z załączników umożliwia rozprzestrzenianie wirusów

Potencjalne zagrożenia systemu pocztowego

- Wiele innych zagrożeń
  - Zagrożenie prywatności: wykrywanie momentu, kiedy poczta jest czytana
  - Wyparcie się wysłania: nadawca może wyprzeć się faktu wysłania konkretnego listu
  - Wyparcie się odbioru: odbiorca może wyprzeć się faktu odebrania konkretnego listu
- ...

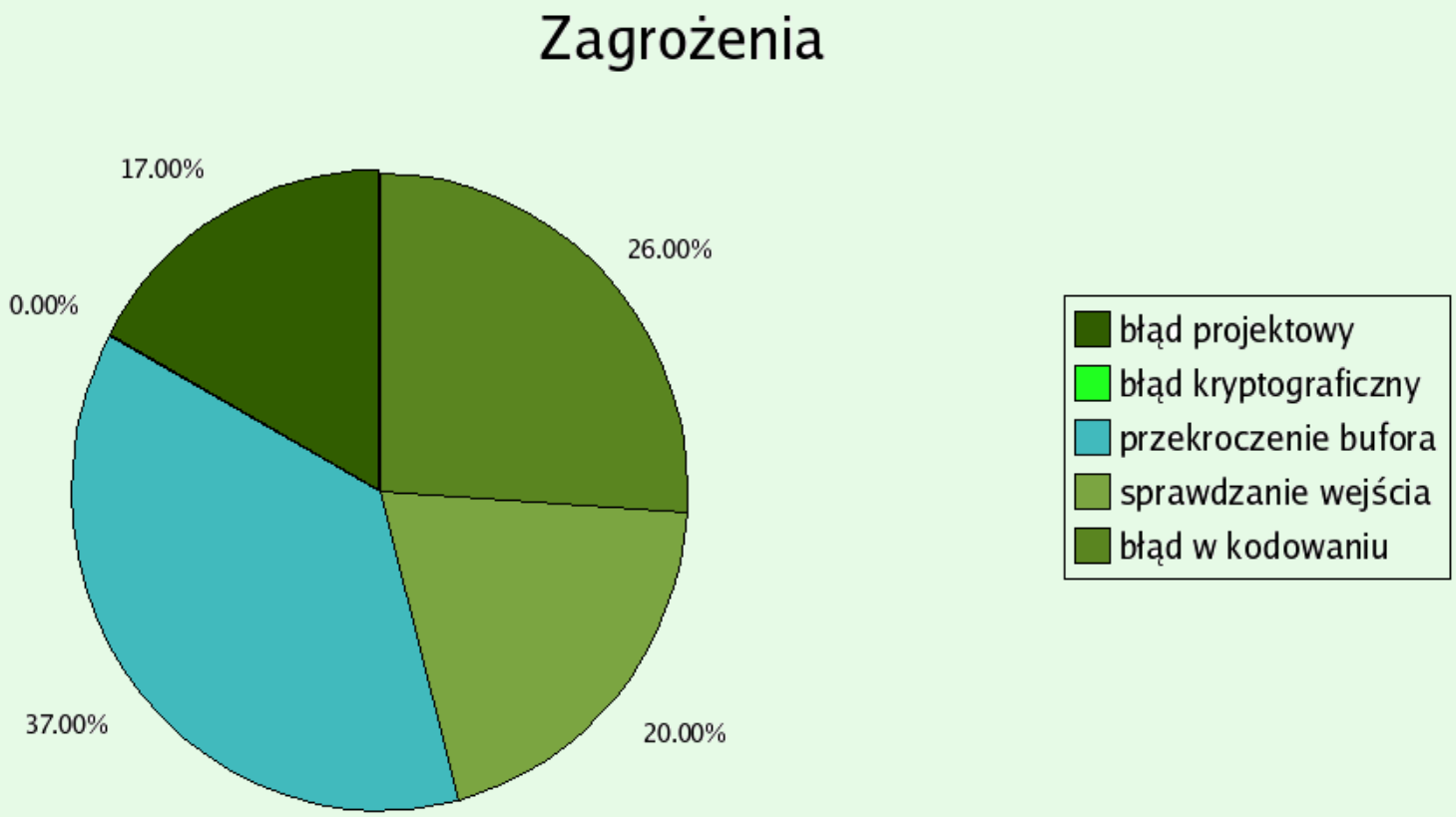
Zagrożenia i luki w bezpieczeństwie

- Kluczowa jest wiedza o zagrożeniach i lukach w bezpieczeństwie
  - pierwsze protokoły sieciowe są z założenia niebezpieczne, bo projektowane były w środowiskach naukowych dla naukowców
- Luki w bezpieczeństwie są zwykle właściwe dla konkretnego
  - języka programowania,
  - systemu operacyjnego,
  - bazy danych,
  - …

Zagrożenia i luki w bezpieczeństwie

- Kluczowa jest wiedza o zagrożeniach i lukach w bezpieczeństwie
- Luki w bezpieczeństwie są zwykle właściwe dla konkretnego systemu
- . . . i wciąż się zmieniają, więc nie można założyć, że kiedyś wszystkie zostaną wyeliminowane
- *Na szczęście* ludzie wciąż popełniają te same błędy i niektóre z nich nigdy nie zaginą: *buffer overflow*

Typowe luki w bezpieczeństwie



Błędy w bezpieczeństwie znalezione w trakcie miesiąca poprawiania błędów w Microsofcie (2002 r.)

Źródła luk w bezpieczeństwie

- Błędy w aplikacjach lub ich infrastrukturze
  - tzn. nie robią, co powinny
- Niewłaściwe własności aplikacji lub infrastruktury
  - tzn. robi coś, czego nie powinna (funkcjonalność przeważa nad bezpieczeństwem)
- Niewłaściwe użycie możliwości aplikacji i infrastruktury
  - złożoność możliwości
  - niedouczenie projektantów i programistów

Funkcjonalność a bezpieczeństwo

- Przegrane bitwy?
  - systemy operacyjne
    - duże projekty, duże pole ataku (API)
  - języki programowania
    - przekroczenia buforów, napisy formatujące itp. w C
    - pola publiczne w Javie
    - tony rzeczy w PHP
  - przeglądarki
    - pluginy,
    - javascript, VPscript,
    - ...
  - programy pocztowe

Java jest bezpieczniejsza

- Nie ma przekroczenia buforów, ale...
  - Można modyfikować system
  - Można naruszać prywatność
  - Można spowodować denial-of-service
  - Można zrobić coś denerwującego
  - Mogą się kryć błędy w maszynie wirtualnej
  - Mogą się kryć błędy w zaprojektowanych mechanizmach
  - Mogą się kryć błędy w implementacji tych mechanizmów