BEZPIECZEŃSTWO SYSTEMÓW KOMPUTEROWYCH

Wykład 7

7. Atak na bezpieczeństwo systemu komputerowego

1. Podstawowe pojęcia i definicje
2. Klasy ataków
3. Formy ataku elektronicznego
4. Fazy ataku elektronicznego
5. Sposoby zmniejszenia podatności na atak
6. Problemy związane z zabezpieczeniem przed atakiem
7. Podstawowe reguły ochrony przed atakiem
8. Proces przydziału praw dostępu
9. Kontrola dostępu do danych
10. Klasy bezpieczeństwa systemów komputerowych

2

7.1. Podstawowe pojęcia i definicje

1. podmiot
2. zasób
3. identyfikacja
4. uwierzytelnianie
5. autoryzacja
6. kontrola dostępu
7. poufność
8. integralność
9. autentyczność
10. niezaprzeczalność
11. prawa dostępu

3

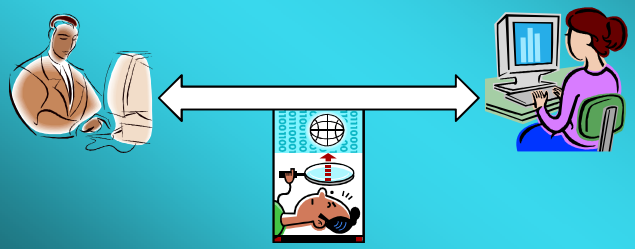
7.2. Klasy ataków

1. Ze względu na rodzaj interakcji pomiędzy atakowanym a atakującym:
   - pasywne
   - aktywne
2. Ze względu na źródło początku ataku:
   - zdalne
   - lokalne

4

7.2. Klasy ataków

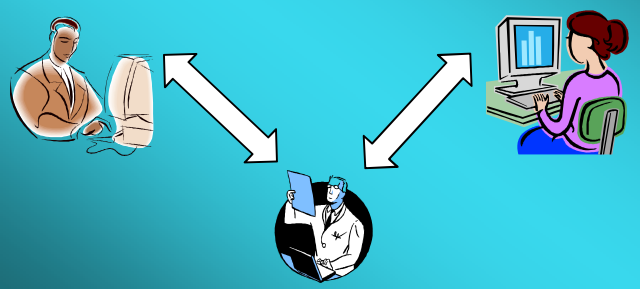
1. **Atak pasywny:**



5

7.2. Klasy ataków

1. **Atak aktywny:**



6

7.3. Formy ataku elektronicznego

- **podszywanie** (masquerading)
- **podsłuch** (eavesdropping)
- **odtwarzanie** (replaying)
- **manipulacja** (tampering)
- **wykorzystywanie luk** (exploiting, penetration)

7

7.3. Formy ataku elektronicznego

Należy pamiętać, że wraz z rozwojem technologii informatycznych ewoluują też sposoby ataków na systemy komputerowe

8

7.3. Formy ataku elektronicznego

Ewolucja ataków na systemy …

	Wykorzystanie trywialnych haseł i znanych luk w programach
	Analiza kodu źródłowego narzędzi systemowych w celu odkrycia luk
1993	Węszenie (ang. sniff), podsłuchiwanie haseł
	Wirusy, konie trojańskie
	Ataki na pocztę elektroniczną
	Ataki poprzez NFS (ang. Network File System) i NIS (ang.Network Information Service)
1995	Podszywanie się (ang. spoofing) pod adres IP lub pod DNS
	Ataki na rutery
1998	Odmowa usługi, DoS (ang. denial of service)
	Przejmowanie stron www (ang. page hijacking)
2000	SPAM – Spiced Pork And haM
	Dialery, malware (adware, spyware)
2002	Łowienie w sieci (ang. web-phishing, personal data fishing)
2005	Ataki na komunikatory (ang. spim, spimming)

9

7.4. Fazy ataku elektronicznego

- skanowanie
- wyznaczenie celu
- atak na system
- modyfikacja systemu
- usuwanie śladów
- propagacja ataku

10

7.5. Zmniejszenie podatności na atak

By zmniejszyć podatność na atak należy chronić wszystkie elementy systemu w tym co najmniej stacje robocze, sieć lokalną i działające usługi sieciowe. Dzięki temu podatność systemu na „typowe” ataki ulega znacznemu ograniczeniu.

11

7.5.1. Zasady ochrony stacji roboczych

- blokada startu systemu z zewnętrznego nośnika
- blokada/ograniczenie możliwości używania zewnętrznych nośników
- rejestracja wszystkich prób dostępu do systemu
- bezpieczne kasowanie poufnych danych
- blokada możliwości wyłączenia zabezpieczeń
- wymuszona i konsekwentna polityka stosowania bezpiecznych haseł użytkowników

12

7.5.2. Zasady ochrony sieci lokalnej

- odpowiedni dobór topologii i okablowania
- fizyczna ochrona infrastruktury IT
- zdefiniowanie listy stanowisk, z których dany użytkownik może uzyskać dostęp do systemu
- blokowanie długo nieużywanych kont użytkowników
- usuwanie kont użytkowników po ustaniu stosunku pracy

13

7.5.3. Zasady ochrony usług sieciowych

- usunięcie z systemu wszystkich usług zbędnych
- zastąpienie usług niezbędnych odpowiednikami o podwyższonym bezpieczeństwie
- kontrola dostępu do pozostałych usług

14

7.6. Problemy związane z zabezpieczeniem przed atakiem

Pamiętajmy, że problemy występujące przy budowie zabezpieczeń stawiają nas (broniących się) w gorszej sytuacji. Atakujących może być wielu, mogą dysponować większymi środkami, zwykle maja więcej czasu i zupełnie inną motywację.

15

7.6.1. Problem związany z asymetrią

- by skutecznie zabezpieczyć system należy usunąć **wszystkie** jego słabości

ale

- by skutecznie zaatakować, wystarczy znaleźć **jedną** słabość

16

7.6.2. Problem związany z otoczeniem

- bezpieczeństwo systemu powinno być rozważane w kontekście całego otoczenia w którym system ten się znajduje
- błędem jest ograniczenie rozważań do pojedynczego systemu

17

7.6.3. Problem związany z zarządzaniem

- dobre zarządzanie zabezpieczeniami systemu to proces ciągły
- błędem jest ograniczenie zabezpieczeń do pojedynczej operacji

18

7.7. Podstawowe reguły ochrony przed atakiem

Aby ograniczyć wpływ wymienionych w poprzednim rozdziale problemów, przy realizacji zabezpieczeń należy zastosować:

- zasadę naturalnego styku z użytkownikiem
- zasadę spójności poziomej i pionowej
- zasadę minimalnego przywileju
- zasadę domyślnej odmowy dostępu

19

7.7.1. Zasada naturalnego styku z użytkownikiem systemu

- zabezpieczenia powinny być postrzegane jako naturalny element systemu
- zabezpieczenia nie mogą utrudniać pracy

20

7.7.2. Zasada spójności

- **poziomej - wymaga aby wszystkie komponenty w danej warstwie systemu zostały zabezpieczone na jednakowym poziomie**
- **pionowej – wymaga by zabezpieczając jedną warstwę przez którą istnieje dostęp do systemu, pamiętać o zabezpieczeniu innych, z których taki dostęp też jest możliwy**

21

7.7.2. Zasada minimalnych przywilejów

- **mająca oparcie w Polityce Bezpieczeństwa**
- **uprawnienia nadawane tylko w takim zakresie jaki jest niezbędny do wykonywania pracy na danym stanowisku**
- **przy zmianie zakresu obowiązków pracownika powinna następować „automatyczna” zmiana zakresu uprawnień**

22

7.7.2. Zasada domyślnej odmowy dostępu

W przypadku gdy mechanizmy obronne systemu nie są w stanie na podstawie wcześniej zdefiniowanych reguł podjąć wynikającej z nich decyzji,

to ostateczną i jedyną prawidłową decyzją powinna być „odmowa dostępu”

23

7.8. Proces przydziału praw dostępu

W procesie przydziału praw dostępu możemy kierować się jedną z zasad:

- **dozwolone jest wszystko**
- **dozwolone jest wszystko co nie jest** (w sposób jawny) **zabronione**
- **zabronione jest wszystko co nie jest** (w sposób jawny) **dozwolone**
- **zabronione jest wszystko**

24

7.9. Kontrola dostępu do danych

Metody kontroli dostępu do danych:

- **DAC (Discretionary Access Control)**
  klasa C
- **MAC (Mandatory Access Control)**
  klasa B
- **RBAC (Role-Based Access Control)**

25

7.9.1. Uznaniowa kontrola dostępu DAC (Discretionary Access Control)

- dane identyfikacyjne i hasła są zabezpieczone przed niepowołanym dostępem
- użytkownicy maja dużą elastyczność i swobodę współdzielenia zasobów - każdy użytkownik ma pełną kontrolę nad obiektami, które stanowią jego własność
- nadanie uprawnień najczęściej reguluje operacje odczytu i zapisu plików oraz uruchomienia programu
- najwięcej problemów wynika z niefrasobliwego nadawania uprawnień (przez zaniedbanie lub nieświadomie) co prowadzi do niewystarczającej ochrony zasobów

26

7.9.2. Obowiązkowa kontrola dostępu MAC (Mandatory Access Control)

- uprawnienia wymuszają automatyczne i precyzyjne reguły dostępu (polityki)
- na podstawie atrybutów bezpieczeństwa i polityk, system operacyjny udziela bądź odmawia podmiotowi dostępu do obiektu
- tylko administrator systemu może ustawiać atrybuty bezpieczeństwa i polityki
- nawet właściciel zasobu nie może dysponować prawami dostępu
- użytkownik nie ma wpływu na działanie mechanizmów kontroli dostępu

27

7.9.3. Kontrola dostępu oparta o role RBAC (Role-Based Access Control)

- w zależności od pełnionych w organizacji funkcji oraz przydzielonych zakresów obowiązków tworzy się tzw. role
- zdefiniowanym rolom są przydzielane stosowne uprawnienia w systemie informatycznym
- następnie role są przypisywane użytkownikom co daje im uprawnienia do wykonywania określonych dla tych ról czynności
- jeden użytkownik może posiadać wiele przypisanych ról oraz jedna rola może być przypisana do wielu użytkowników

28

7.10.1. Klasy bezpieczeństwa systemów komputerowych

Gdzie i kiedy powstały reguły klasyfikacji systemów:

- Trusted Computer System Evaluation Criteria (Orange book) opracowany w USA stał się światowym standardem i obowiązywał w latach 1983-2000; do dzisiaj znajdujemy odwołania do tego standardu; stał się inspiracją do opracowania podobnych norm także w Europie; oryginalny dokument dostępny jest pod adresem http://csrc.nist.gov/publications/history/dod85.pdf

29

7.10.1. Klasy bezpieczeństwa systemów komputerowych

- D - ochrona minimalna (Minimal Protection)
- C1 - ochrona uznaniowa (Discretionary Protection)
- C2 - ochrona z kontrolą dostępu (Controlled Access Protection)
- B1 - ochrona z etykietowaniem (Labeled Security Protection)
- B2 - ochrona strukturalna (Structured Protection)
- B3 - ochrona przez podział (Security Domains)
- A1 - konstrukcja zweryfikowana (Verified Design)

30

7.10.1. Klasy bezpieczeństwa systemów komputerowych

Przy klasyfikowaniu bezpieczeństwa wg. TCSEC należy pamiętać, że klasa wyższa zawiera wszystkie wymagania klasy niższej.

np. klasa C2 zawiera wymagania klasy C1 i dodatkowo mechanizmy umożliwiające audyt i śledzenie operacji użytkowników oraz wykorzystania zasobów

31

7.10.2. Klasy bezpieczeństwa systemów komputerowych

- Information Technology Security Evaluation Criteria (ITSEC) opracowany wspólnie przez Francję, Niemcy, Holandię i Wielką Brytanię w 1990 roku; powstał głównie z angielskiego CESG2/DTIEC, francuskiego SCSSI oraz niemieckiego ZSIEC; kolejna wersja została opublikowana przez Komisję Europejską w 1991 roku; oryginalny dokument dostępny jest pod adresem: http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf

32

7.10.3. Klasy bezpieczeństwa systemów komputerowych

- **Common Criteria Assurance Levels (od 1999 roku zaakceptowany jako norma ISO 15408) od 1996 roku znany jako Common Criteria for Information Technology Security Evaluation ; powstał z ITSEC, TCSEC i CTCPEC** (Kanada)**; oryginalny dokument dostępny jest pod adresem: http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3.pdf**

33

7.10.3. Klasy bezpieczeństwa systemów komputerowych

Poziomy pewności EAL (według CC):

EAL0: brak pewności.

EAL1: produkt testowany funkcjonalnie, analiza bezpieczeństwa wykorzystująca specyfikację funkcji interfejsu w celu zrozumienia zachowania systemu, niezależne testowanie funkcji bezpieczeństwa

EAL2: produkt testowany strukturalnie, analiza bezpieczeństwa wykorzystująca wysokopoziomowy opis projektu podsystemów, dowody testowania przez producenta wyszukiwania oczywistych słabych punktów

34

7.10.3. Klasy bezpieczeństwa systemów komputerowych

Poziomy pewności EAL (według CC):

EAL3: produkt testowany metodycznie sprawdzany, analiza bezpieczeństwa wykorzystująca metodę selektywnego i niezależnego potwierdzenia wyników (tzw. „szarej skrzynki") testów producenta, wymagania związane ze środowiskiem produkcji i zarządzaniem konfiguracją

EAL4: produkt metodycznie projektowany, testowany sprawdzany, analiza bezpieczeństwa wykorzystująca niskopoziomowy projekt modułów systemu, niezależne wyszukiwanie luk w systemie, model życia, automatyczne zarządzanie konfiguracją

35

7.10.3. Klasy bezpieczeństwa systemów komputerowych

Poziomy pewności EAL (według CC):

EAL5: produkt projektowany półformalnie testowany, pełna analiza implementacji, pewność na podstawie modelu formalnego półformalnej prezentacji specyfikacji funkcjonalnej wysokopoziomowego opisu, poszukiwanie luk musi wykazać względną odporność na atak penetracyjny, detekcja i analiza ukrytych kanałów, modularność projektu

36

7.10.3. Klasy bezpieczeństwa systemów komputerowych

Poziomy pewności EAL (według CC):

EAL6: produkt z projektem półformalnie weryfikowanym testowany, projektowanie modularne, warstwowe, poszukiwanie luk musi wykazać wysoką odporność na atak penetracyjny, systematyczna detekcja i analiza ukrytych kanałów, zaostrzone rygory środowiska produkcji i zarządzania konfiguracją

37

7.10.3. Klasy bezpieczeństwa systemów komputerowych

Poziomy pewności EAL (według CC):

EAL7: produkt z projektem formalnie weryfikowanym testowany, formalne podejście do specyfikowania, projektowania dokumentowania systemu, kompletne niezależne testowanie i weryfikacja testów producenta, minimalizacja złożoności projektu

38

7.10.3. Klasy bezpieczeństwa systemów komputerowych

Poziomy pewności EAL (według CC):

EAL7: produkt z projektem formalnie weryfikowanym testowany, formalne podejście do specyfikowania, projektowania dokumentowania systemu, kompletne niezależne testowanie i weryfikacja testów producenta, minimalizacja złożoności projektu

39

7.10.4. Klasy bezpieczeństwa systemów komputerowych

Porównanie klas bezpieczeństwa

TCSEC	ITCES	CC / EAL
D	E0	EAL0
		EAL1
C1	E1, F-C1	EAL2
C2	E2, F-C2	EAL3
B1	E3, F-B1	EAL4
B2	E4, F-B2	EAL5
B3	E5, F-B3	EAL6
A1	E6, F-B3	EAL7

40

7.10.4. Klasy bezpieczeństwa systemów komputerowych

Przynależność systemów do klas

D	C1	C2	B1	A1
EAL0/1	EAL2	EAL3	EAL4	EAL7
Win 9x	Unix, Linux, NetWare	Solaris, AIX, Windows NT	Trusted Solaris, Trusted IRIX HP-UX, Ultrix, SuSE Linux(4+), Win 2k Prof.SP3	SCC Secure Network Server, Gemini Trusted Network Processor

Czy są …

jakieś pytania ?