# Bezpieczeństwo w sieci lokalnej - prezentacja na potrzeby Systemów operacyjnych

Tomasz Warchoł

Wydział Matematyki, Informatyki i Mechaniaki
Uniwersytet Warszawski

Warszawa, 16 stycznia 2007

# Zarys wstępu do wprowadzenia

- Pakiety - wszystko pływa losowo w małych kawałkach

Każdy komunikat przsyłany jest we fragmentach, zwanych pakietami. Pakiet zawiera nagłówek, w którym znajdują się między innymi informacje o nadawcy i odbiorcy komunikatu oraz typ pakietu; oraz treść, czyli fragment komunikatu. Treść może być zakodowana lub nie, w zależności od typu pakietu.

# Zarys wstępu do wprowadzenia

- Pakiety - wszystko pływa losowo w małych kawałkach
- Komunikacja w sieci - jeden mówi, reszta słucha

Komunikacja w sieci lokalnej, w której wszystkie komputery mają dostęp do jednego ośrodka (np. sieć w topologii gwiazdy) jest "jednowątkowa". W danym momencie tylko jeden komputer wysyła pakiety do ośrodka. Pozostałe odbierają wysłany pakiet, analizują go po czym zaczyna nadawać kolejny komputer.

# Zarys wstępu do wprowadzenia

- Pakiety - wszystko pływa losowo w małych kawałkach
- Komunikacja w sieci - jeden mówi, reszta słucha
- Łączenie podsieci

W sieciach bardziej złożonych stosuje się urządzenia łączące ośrodki. Działają one jak przekaźniki odbierające pakiety z jednej gałęzi sieci i transmitujące je do drugiej.

# Zarys wstępu do wprowadzenia

- Pakiety - wszystko pływa losowo w małych kawałkach
- Komunikacja w sieci - jeden mówi, reszta słucha
- Łączenie podsieci
  - Koncentrator

Koncentrator odbiera pakiety z jednej gałęzi i wysyła je do wszystkich innych. Sieć z koncentratoren działa tak, jakby wszystkie ośrodki były połączone w jeden.

# Zarys wstępu do wprowadzenia

- Pakiety - wszystko pływa losowo w małych kawałkach
- Komunikacja w sieci - jeden mówi, reszta słucha
- Łączenie podsieci
  - Koncentrator
  - Switch

Switch analizuje ruch w sieci i przesyła pakiet tylko do tej gałęzi, w której jest jego odbiorca. W sieci takiej jest niezależna komunikacja pomiędzy wszystkimi gałęziami.

# Zarys wstępu do wprowadzenia

- Pakiety - wszystko pływa losowo w małych kawałkach
- Komunikacja w sieci - jeden mówi, reszta słucha
- Łączenie podsieci
  - Koncentrator
  - Switch

**PAMIĘTAJ!**

Sieć NIE JEST bezpieczna!

# Sniffery

- Co to jest?

Sniffer to urządzenie lub program, którego celem jest przechwytywanie pakietów krążących w sieci bez względu na to, do kogo są adresowane.

# Sniffery

- Co to jest?

Każda karta sieciowa może działać w dwóch trybach: normalnym, kiedy odbiera tylko pakiety do niej skierowane, lub tzw. "nasłuchu", kiedy odbiera wszystkie pakiety do niej docierające. Przestawienie karty w tryb "nasłuchu" wymaga praw root'a.

# Sniffery

- Co to jest?
- tcpdump

*tcpdump* to program, który wyświetla wszystkie pakiety docierające do karty sieciowej. Nie potrafi analizować pakietów, wyświetla tylko informacje o nagłówku i treść w kodzie ASCII lub szesnastkowym.

# Sniffery

- Co to jest?
- tcpdump
- dsniff

*dsniff* to pakiet narzędzi do podsłuchiwania ruchu sieciowego. Są to wyspecjalizowane programy o bardzo konkretnym zastosowaniu, ale działające dla szerokiej klasy sieci i typów pakietów. Przykłady to programy *dsniff* do wychwytywania haseł z nieszyfrowanych pakietów, oraz *arpspoof* do przekierowywania ruchu w sieci.

# Sniffery

- Co to jest?
- tcpdump
- dsniff
- Dlaczego chcemy switch'a?

Dzięki inteligentnemu przekierowywaniu pakietów switch ogranicza ilość komputerów, na których można uprawiać pasywny nasłuch.

# Sniffery

- Co to jest?
- tcpdump
- dsniff
- Dlaczego chcemy switch'a?
- Dlaczego switch nam nie pomoże?

Różne rodzaje "fałszywych" pakietów mogę przekonać sieć lub switch'a, że trasa pakietu jest inna od planowanej.

# Sniffery

- Co to jest?
- tcpdump
- dsniff
- Dlaczego chcemy switch'a?
- Dlaczego switch nam nie pomoże?
  - MAC flooding

Switch pamięta lokalizacje konkretnych komputerów w skończonej tablicy. Gdy przepełnimy tablicę, zaczyna się zwykle zachowywać jak koncentrator i wysyła "wszystko do wszystkich".

# Sniffery

- Co to jest?
- tcpdump
- dsniff
- Dlaczego chcemy switch'a?
- Dlaczego switch nam nie pomoże?
  - MAC flooding
  - ARP spoofing

Aby komputer mógł połączyć się z innym w sieci, musi znać adres MAC jego karty. Wysyła pakiet z zapytaniem. Jeżeli wyślemy fałszywy pakiet z odpowiedzią, atakowany komputer będzie wysyłał pakiety dowolną trasą.

# Sniffery

- Co to jest?
- tcpdump
- dsniff
- Dlaczego chcemy switch'a?
- Dlaczego switch nam nie pomoże?
  - MAC flooding
  - ARP spoofing
  - ARP poisoning

Jeżeli komputer dostaje pakiet z zapytaniem o adres MAC, to zapamiętuje adres MAC nadawcy. Wysyłając fałszywe zapytania możemy dowolnie manipulować trasami pakietów wysyłanych z danego komputera.

Na atakowanym komputerze uruchamiamy program dsniff. Program wypisuje na konsolę wszystkie przechwycone czystym tekstem loginy i hasła znajdujące się w pakietach docierających bezpośrednio do karty sieciowej. Sprawdzamy, że "hakerowanie" jest łatwe na następujących protokołach:

- ftp

- ftp
- telnet

- ftp
- telnet
- http

Używając programu arpspoof przekierowujemy pakiety krążące pomiędzy dowolnym komputerem a bramą naszej sieci tak, aby przechodziły przez nsz komputer. Możemy teraz podsłuchać wszystkie komunikaty pomiędzy "ofiarą" a światem.

- ftp
- telnet
- http
- gadu-gadu

- ftp
- telnet
- http
- gadu-gadu
- inne: SMTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL*Net, Sybase, Microsoft SQL protocols

# Jak się przed tym bronić?

- anty-sniffery

*anty-sniffer* to program lub urządzenie wyszukujące sniffery. Ponieważ sniffery często nie ingerują w sieć, wykrycie ich jest trudne. Najczęściej wykorzystywana metoda to wysyłanie pewnych spreparowanych pakietów, których żadna normalna karta sieciowa nie powinna przyjąć. Przyjmie je tylko karta w trybie "nasłuchu".

# Jak się przed tym bronić?

- anty-sniffery
- analiza ruchu w sieci

Jeżeli sniffer zmienia trasy pakietów, to można czasem to wykryć analizując ruch w sieci i tworząc schematy na różne okresy aktywności sieci. Odstępstwo od tych schematów może oznaczać pracę sniffera.

# Jak się przed tym bronić?

- anty-sniffery
- analiza ruchu w sieci
- szyfrowanie

**PAMIĘTAJ!**

Szyfrowanie Twoim przyjacielem jest!

Jedyną w pełni skuteczną metodą uchronienia się przez wyciekiem informacji jest uniemożliwienie analizy pakietu przez jego zaszyfrowanie.

# PKI

- PK - Public Key

*Public Key* to ogólna nazwa systemów kryptograficznych, w których szyfrowanie/podpisywanie/uwierzytelnianie odbywa się za pomocą danych podanych do wiadomości publicznej, natomiast operacja odwrotna przy pomocy tajnych danych znanych tylko tworzącemu system.

# PKI

- PK - Public Key
- PKI - Public Key Infrastructure

*PKI* to mrzonka o kryptosystemie, w którym każdy użytkownik posiada swój zatwierdzony klucz publiczny i wszelka komunikacja z nim przy pomocy tego klucza jest bezpieczna. PKI nie może istnieć, bo nie istnieje podmiot który mógłby uwierzytelnić każdego użytkownika.

# PKI

- PK - Public Key
- PKI - Public Key Infrastructure
- Certyfikaty

Certyfikaty to praktyczna próba implementacji namiastki PKI. "Wystawca" wydaje użytkownikom certyfikaty, które potwierdzają pewne dane, np. certyfikat tożsamości serwera.

# SSL - Secure Socket Layer

- SSL - Secure Socket Layer
  - prywatność
  - uwierzytelnianie
  - integralność

*SSL* to protokół umożliwiający zabezpieczenie transmisji w sieci. Parametry protokołu, jak np. algorytmy szyfrujące, są uzgadniane przez strony na początku transmisji w trakcie tzw. Handshake.

# SSL - Secure Socket Layer

- SSL - Secure Socket Layer
  - prywatność
  - uwierzytelnianie
  - integralność
- TLS - Transport Layer Security

*TLS* to rozwinięcie SSL, jeszcze bezpieczniejsze i bardziej niezawodne.

# Handshake

- $C \rightarrow S$ dane o SSL, losowe dane

# Handshake

- $C \rightarrow S$ dane o SSL, losowe dane
- $C \leftarrow S$ dane o SSL, certyfikat

# Handshake

- $C \rightarrow S$ dane o SSL, losowe dane
- $C \leftarrow S$ dane o SSL, certyfikat
- $C \rightarrow S$ uwierzytelnienie servera, premaster key

# Handshake

- $C \rightarrow S$ dane o SSL, losowe dane
- $C \leftarrow S$ dane o SSL, certyfikat
- $C \rightarrow S$ uwierzytelnienie servera, premaster key
- S i C generują master key

# Handshake

- $C \rightarrow S$ dane o SSL, losowe dane
- $C \leftarrow S$ dane o SSL, certyfikat
- $C \rightarrow S$ uwierzytelnienie servera, premaster key
- S i C generują master key
- $C \rightarrow S$ end of handshake

# Handshake

- $C \rightarrow S$ dane o SSL, losowe dane
- $C \leftarrow S$ dane o SSL, certyfikat
- $C \rightarrow S$ uwierzytelnienie servera, premaster key
- S i C generują master key
- $C \rightarrow S$ end of handshake
- $S \leftarrow C$ end of handshake

# Kryptografia w SSL

Najczęściej używane algorytmy w SSL:

- PK – RSA, Diffie-Hellman, DSA, Fortezza
- szyfrowanie – RC2, RC4, IDEA, DES, Triple DES, AES, Camellia
- hashowanie – MD2, MD4, MD5, SHA-1, SHA-2

# Kryptografia w SSL

Najczęściej używane algorytmy w SSL:

- PK – RSA, Diffie-Hellman, DSA, Fortezza
- szyfrowanie – RC2, RC4, IDEA, DES, Triple DES, AES, Camellia
- hashowanie – MD2, MD4, MD5, SHA-1, SHA-2

Zaznaczone algorytmy NIE są bezpieczne. Złamano je, lub ujawniono poważne słabości które mogą ułatwić ataki. Samo SSL nie wystarczy, trzeba też używać bezpiecznych algorytmów.

# Bibliografia


- http://www.surasoft.com/articles/packetsniffing.php
- http://www.monkey.org/ dugsong/dsniff/
- http://www.pki-page.org/