

# **Bezpieczeństwo protokołów sieciowych na przykładzie TCP/IP.**

## **Wstęp.....4**

### **Rozdział 1**

#### **Analiza zagadnienia**

2.1 Niebezpieczeństwa przesyłania danych przez sieci.....4

2.2 Ochrona danych przesyłanych przez internet.....5

2.3 Model OSI .....6

2.4 Model TCP/IP.....8

### **Rozdział 2**

**Bezpieczeństwo na poziomie poszczególnych warstw.....10**

### **Rozdział 3**

#### **Warstwa fizyczna**

4.1 Zagrożenia w warstwie fizycznej.....11

4.1.1 Zastosowanie metod kryptograficznych.....11

4.1.2 Bezpieczeństwo okablowania sieciowego.....11

4.1.3 Sprzęt sieciowy.....12

### **Rozdział 4**

#### **Warstwa internetowa.**

5.1 Internet Protocol Security (IPSEC) .....14

5.1.1 Authentication Header.....15

5.1.2 Encapsulating Security Payload.....16

5.1.3 Tryb pracy protokołów IPsec.....18

5.1.4 Zarządzenie kluczem.....19

5.1.5 Schemat działania IPsec.....20

5.1.5.1 Działania wykonywane przy wysyłaniu pakietu .....21

5.1.5.2 Działania wykonywane przy odbieraniu pakietu .....22

5.1.6 Mechanizmy kryptograficzne używane przez protokołu IPsec

|   |         |
|---|---------|
| .....   | 22      |
| 5.1.6.1 HMAC                                    | 22      |
| 5.1.6.2 DES, Diffie-Hellman, DSA, SHA, RSA, MD5 | .....23 |
| 5.2 IP WERSJA 6 (IPV6)                          | 24      |
| 5.2.1 Zmiany w porównaniu z IPv4.....           | 24      |
| 5.2.2 Cechy IPv6.....                           | 25      |

## **Rozdział 5**

### **Warstwa transportowa**

|   |         |
|---|---------|
| 6.1 Secure Sockets Layer.....                     | 28      |
| 6.1.1 Zadania SSL.....                            | 28      |
| 6.1.2 Architektura i działanie protokołu SSL..... | 29      |
| 6.1.2.1 SSL Handshake Protocol.....               | 30      |
| 6.1.2.2 SSL Record Protocol.....                  | 32      |
| 6.2 Secure shell.....                             | 33      |
| 6.3 Transport layer security                      | .....35 |

## **Rozdział 6**

### **Warstwa aplikacji.**

|  |    |
|--|----|
| 7.1 Poczta elektroniczna.....                      | 36 |
| 7.1.1 S/MIME.....                                  | 36 |
| 7.1.2 Pretty Good Privacy.....                     | 37 |
| 7.2 Uwierzytelnianie, autoryzacja i logowanie..... | 37 |

## **Rozdział 7**

### **Konfiguracja i zastosowanie IPSEC.**

|   |    |
|---|----|
| 8.1 Protokół IPSEC w systemach Windows..... | 39 |
| 8.2 Zastosowanie protokołu IPSEC.....       | 40 |
| 8.3 Działanie IPSEC w Windows.....          | 41 |
| 8.3.1 Filtry.....                           | 41 |
| 8.3.2 Reguły filtrowania.....               | 41 |
| 8.3.3 Akcje.....                            | 42 |
| 8.3.4 Zasady.....                           | 42 |

## **Rozdział 8**

### **Konfiguracja IPSEC.**

|  |    |
|--|----|
| 9.1 Dodanie przystawki z zasada bezpieczeństwa do MMC..... | 43 |
|--|----|

|         |   |    |
|---------|---|----|
| 9.1.1.1 | Utworzenie zasady bezpieczeństwa IPSec.....       | 46 |
| 9.1.1.2 | Dodawanie reguł filtrowania do zasad.....         | 48 |
| 9.1.1.3 | Dodawanie listy filtrów do reguł filtrowania..... | 50 |
| 9.1.1.4 | Zakończenie konfigurowania reguły .....           | 52 |
| 9.1.1.5 | Modyfikacja zasad IPSec.....                      | 54 |
| 9.1.1.6 | Sprawdzenie typu połączenia naszej reguły.....    | 55 |
| 9.1.1.7 | Włączanie zasady IPSec.....                       | 56 |
| 9.1.1.8 | Monitorowanie zabezpieczeń protokołu IPSec .....  | 56 |
| 9.2     | Blokowanie ruchu za pomocą IPSEC.....             | 57 |

## **IPSEC Podsumowanie .....**

|      |                             |    |
|------|-----------------------------|----|
| 10.1 | IPSEC – wady i zalety ..... | 64 |
| 10.2 | Aktualne tendencje .....    | 65 |

## **11 Wykaz oznaczeń i skrótów.....**

## **12 Bibliografia .....**