

Podpis cyfrowy i identyfikacja użytkowników w sieci Internet / A. Grzywak [et al.]. – Dąbrowa Górnicza, 2013

Spis treści

1. Wstęp	9
2. Algorytmy kryptograficzne	11
2.1. Szyfrowanie symetryczne	11
2.1.1. Data Encryption Standard - algorytm DES	11
2.1.2. Działanie algorytmu AES	17
2.2. Szyfrowanie asymetryczne	21
2.2.1. Algorytm RSA	22
2.2.2. Algorytm DSA	24
2.3. Funkcje skrótu	25
2.3.1. Algorytm MD5	26
2.3.2. Algorytm rodziny SHA	29
3. Rozwój metod uwierzytelniania użytkownika sieci	34
3.1. Podpis elektroniczny oparty o symetryczne algorytmy kryptografii	35
3.2. Tworzenie i weryfikacja podpisu cyfrowego w technice asymetrycznej	36
3.3. Dystrybucja klucza	39
3.4. Modele zaufania	42
4. Protokoły komunikacyjne podwyższające bezpieczeństwo informacji w sieciach	45
4.1. Konstrukcja wirtualnych sieci prywatnych VPN	47
4.1.1. Rodzaje i klasyfikacja sieci VPN	49
4.1.2. Klasyfikacje sieci VPN	50
4.2. Protokół IPSEC	53
4.2.1. Protokoły bezpieczeństwa IPsec	55
4.2.2. Rozwój i przyszłość IPsec	58
4.2.3. SSTP jako przykład kontrtechnologii dla IPsec	58
4.2.4. Podsumowanie	59
4.3. Protokoły SSL/TLS	59
4.3.1. Zasada działania SSL	60
4.3.2. Zasada działania TLS	62
4.3.3. Dodatkowe informacje o bezpieczeństwie SSL i TLS	66
4.3.4. Porównanie protokołów SSL v2, SSL v3 i TLS	66
4.3.5. Możliwe problemy protokołów SSL oraz TLS	66
4.4. Inne protokoły bezpiecznej komunikacji. Protokół SSH	67
4.4.1. Architektura i zasada działania SSH	68
4.4.2. Bezpieczeństwo SSH	68

5. Zaawansowane metody potwierdzania tożsamości użytkownika	70
5.1. Zastosowanie standardu OpenID w zarządzaniu tożsamością użytkowników	71
5.2. Sprzętowe metody potwierdzania tożsamości użytkownika	74
5.3. Dalszy rozwój rozwiązań OpenID	80
6. Platforma ePUAP i profil zaufany w potwierdzaniu tożsamości użytkowników i podpisywaniu dokumentów elektronicznych	82
6.1. Integracja systemów zewnętrznych z platformą ePUAP	86
6.2. Wymiana danych za pomocą protokołu SAML	87
6.3. Komunikacja systemów zewnętrznych z platformą ePuap	90
6.3.1. Modele komunikacji	91
6.4. Popularyzacja i wykorzystanie profilu zaufanego	92
7. Systemy bezpieczeństwa poczty PGP	94
7.1. Historia PGP	94
7.2. Działanie i bezpieczeństwo PGP	96
7.3. Narzędzia umożliwiające pracę z PGP i GPG	99
7.4. Przekazywanie kluczy dla potrzeb PGP	101
7.5. Zalety wykorzystania PGP w ochronie poczty elektronicznej	102
8. Podpis cyfrowy i bezpieczeństwo IT w aktach prawnych	104
8.1. Usługi systemów kryptograficznych	104
8.2. Podpis elektroniczny w świetle postanowień prawnych Unii Europejskiej	105
8.3. Standaryzacja ogólnoeuropejskiej struktury podpisu elektronicznego	108
8.4. Standardy bezpieczeństwa w systemach IT	113
9. Kryptografia kwantowa w sieciach komputerowych	126
9.1. Uwierzytelnianie użytkowników w protokołach kwantowej dystrybucji klucza	126
9.2. Protokół BB84	130
9.3. Protokół B92	132
9.4. Protokół SARG	134
9.5. Protokół teleportacji kwantowej	137
9.6. Kwantowa korekcja błędów	142
10. Wnioski końcowe	143
11. Literatura	144