

UNIVERSITATEA DIN BACĂU
FACULTATEA DE INGINERIE

POPA SORIN EUGEN

SECURITATEA SISTEMELOR
INFORMATICE

note de curs și aplicații
pentru studenții Facultății de Inginerie



Editura Alma Mater
Universitatea din Bacău

2007

Cuprins

1. NOȚIUNI PRIVIND SECURITATEA INFORMAȚIILOR	5
1.1. INTRODUCERE	5
1.2. DEFINIREA NOȚIUNII DE SECURITATEA INFORMAȚIILOR.....	6
1.3. SECȚIUNILE STANDARDULUI DE SECURITATE ISO / IEC 17799.....	9
1.3.1. <i>Politica de securitate</i>	9
1.3.2. <i>Organizarea securității</i>	9
1.3.3. <i>Clasificarea și controlul activelor</i>	10
1.3.4. <i>Securitatea personalului</i>	10
1.3.5. <i>Securitatea fizică</i>	11
1.3.6. <i>Managementul comunicațiilor și al operării</i>	11
1.3.7. <i>Controlul accesului</i>	13
1.3.8. <i>Dezvoltarea și întreținerea sistemului</i>	14
1.3.9. <i>Planificarea continuității afacerii</i>	15
1.3.10. <i>Conformitatea</i>	15
2. CLASIFICAREA INFORMAȚIILOR	16
2.1. NOȚIUNI INTRODUCTIVE PRIVIND CLASIFICAREA MODERNĂ A INFORMAȚIILOR	16
2.2. CLASIFICAREA INFORMAȚIILOR.....	17
2.2.1. <i>Informațiile subiective</i>	17
2.2.2. <i>Informații obiective</i>	17
2.2.3. <i>Determinarea necesității clasificării informațiilor</i>	18
2.3. DECLASIFICAREA ȘI DEGRADAREA INFORMAȚIILOR CLASIFICATE	19
2.4. PRINCIPIILE PROTEJĂRII INFORMAȚIILOR SPECIALE	20
2.5. PROTEJAREA MEDIILOR DE STOCARE A INFORMAȚIILOR.....	21
2.5.1. <i>Marcarea materialelor cu regim special</i>	21
2.5.2. <i>Păstrarea și distrugerea mediilor de păstrare a informațiilor</i>	22
2.6. CLASIFICAREA INFORMAȚIILOR ORGANIZAȚIILOR.....	22
2.6.1. <i>Criterii de clasificare a informațiilor la nivelul organizațiilor</i>	23
2.6.2. <i>Proceduri de clasificare a informațiilor</i>	23
2.6.3. <i>Roluri și responsabilități în procesul de clasificare a informațiilor</i>	24
3. CONTROLUL ACCESULUI ÎN SISTEMELE INFORMATICE.....	25
3.1. TIPURI DE CONTROL AL ACCESULUI ÎN SISTEM	25
3.1.1. <i>Modele de control al accesului</i>	25
3.1.2. <i>Forme combinate de control</i>	26
3.2. IDENTIFICAREA ȘI AUTENTIFICARE	27
3.2.1. <i>Principiile de bază ale controlului accesului</i>	28
4. CRIPTOGRAFIA	32
4.1. DEFINIȚII ȘI NOȚIUNI DE BAZĂ.....	32
4.1.1. <i>Tehnici utilizate în criptografie</i>	33
4.1.1.1. <i>Substituția</i>	33
4.1.1.2. <i>Permutarea sau transpoziția</i>	35
4.1.1.3. <i>Cifrul lui Vernam</i>	35
4.1.1.4. <i>Ascunderea informațiilor</i>	36
4.1.1.4.1. <i>Steganografia</i>	36
4.1.1.4.2. <i>Filigranarea</i>	37
4.1.1.4.3. <i>Securitatea în domeniul tipăriturilor</i>	37
4.1.2. <i>SISTEME DE CRIPTARE PRIN CHEI SIMETRICE (PRIVATE)</i>	39
4.1.3. <i>SISTEME DE CRIPTARE PRIN CHEI ASIMETRICE (PUBLIC)</i>	40

4.3.1. Semnătura digitală.....	41
4.3.2. Sisteme de certificare a cheilor publice.....	42
4.3.3. Infrastructura cheilor publice (PKI).....	43
5. MODELE ȘI PROGRAME DE SECURITATE.....	44
5.1. MODELE DE SECURITATE MULTINIVEL.....	44
5.1.1. Modelul Bell-LaPadula.....	44
5.1.2. Modelul matricei de control al accesului.....	45
5.1.3. Modelul Biba.....	45
5.2. MODELE ALE SECURITĂȚII MULTILATERALE.....	47
5.3. PROGRAMUL DE SECURITATE.....	49
5.3.1. Politicile de securitate.....	49
5.3.2. Standardele, normele și procedurile de securitate.....	51
5.3.3. Aspecte practice ale politicii de securitate informațională.....	52
5.3.4. Exemple de politici de securitate.....	53
6 SECURITATEA REȚELOR DE CALCULATOARE.....	59
6.1 MECANISME UTILIZATE ÎN SECURIZAREA REȚELOR.....	59
6.1.1 Funcționarea DHCP.....	59
6.1.2 Noțiuni privind securizarea rețelei.....	60
6.1.3 Firewalls.....	61
6.1.4 Proxy-uri.....	63
6.1.5 Filtrele de pachete.....	65
6.2 REȚELE VPN.....	65
6.2.1 Point-to-Point Tunneling Protocol (PPTP).....	66
6.2.2 Layer 2 Tunneling Protocol (L2TP).....	67
6.2.3 IPsec.....	68
7. TEHNICI, SERVICII ȘI SOLUȚII DE SECURITATE PENTRU INTRANET-URI ȘI PORTALURI.....	69
7.1. INTRODUCERE.....	69
7.2. CRIPTOGRAFIA.....	69
7.2.1. Criptografia cu cheie secretă.....	70
7.2.2. Criptografia cu cheie publică.....	70
7.2.3. Managementul cheilor și distribuția acestora.....	70
7.2.4. Funcțiile Hash.....	71
7.2.5. Utilizarea semnăturilor digitale. Riscuri de securitate.....	72
7.2.6. Certificate digitale. Riscuri de securitate.....	73
7.2.7. Autentificarea Kerberos V5.....	75
7.2.7.1. Cum funcționează Kerberos V5.....	76
7.2.7.2. Riscuri de securitate în Kerberos.....	76
7.2.8. Autentificarea SSL/TLS.....	77
7.2.8.1. Legătura SSL-HTTP.....	78
7.2.8.2. Cum funcționează SSL.....	78
7.2.8.3. Performanța SSL.....	79
7.2.8.4. Riscuri de securitate în SSL.....	80
7.2.9. Autentificarea NTLM.....	80
7.2.10. Comparatie Kerberos - NTLM.....	80
7.2.11. SSH.....	81
7.2.11.1. Autentificarea prin SSH.....	82
7.2.11.2. SSH1.....	83
7.2.11.3. SSH 2.....	83
7.2.11.4. Algoritmii de criptare utilizați.....	83
7.2.11.5. Ce poate proteja SSH. Riscuri de securitate ale SSH.....	84
7.2.12. PGP. Riscuri de securitate.....	84

7.2.13. S/MIME.....	86
7.2.13.1. Funcționarea S/MIME	87
7.2.13.2. Riscuri de securitate ale S/MIME	88
7.2.14. Utilizarea firewall-urilor în intraneturi.....	88
8. STRATEGII DE ACHIZIȚIE PENTRU APĂRARE.....	90
8.1. INTRODUCERE	90
8.2. STRATEGII DE SECURITATE ALE RĂZBOIULUI INFORMAȚIONAL	91
Aplicații practice	
L1 CRIPTAREA CA METODĂ DE SECURITATE A INFORMAȚIILOR.....	95
1.1 OBIECTIVE:	95
1.2 CIFRUL LUI CĂZAR	95
1.3 CIFRUL LUI VERNAM.....	97
1.4 METODĂ PROPRIE DE CRIPTARE	97
1.5 DESFĂȘURAREA LUCRĂRII	98
L2 STEGANOGRAFIA CA METODĂ DE SECURITATE A INFORMAȚIILOR.....	99
2.1 OBIECTIVE:	99
2.2 INTRODUCERE	99
2.3 ASCUNDEREA UNUI FIȘIER.....	100
2.4 DESCOPERIREA UNUI FIȘIER ASCUNS	101
L3 FIREWALL-URI.....	102
3.1 OBIECTIVE:	102
3.2 GENERALITĂȚI/DEFINIȚII FIREWALL.....	102
3.2.1 Funcționarea firewall-urilor.....	102
3.2.2 Politica Firewall-ului	103
3.2.3 Clasificări	103
3.2.4 Ce "poate" și ce "nu poate" să facă un firewall?.....	104
3.3 INFORMAȚII DESPRE FIREWALL SUN WINDOWS XP	104
3.3.1 Cum încep să utilizez un firewall?	104
3.3.2 Cum aflu ce versiune de Windows utilizez?	104
3.3.3 Verificarea stării Windows Firewall	105
3.3.4 Adăugarea unei excepții în Windows Firewall.....	105
3.3.5 Probleme de compatibilitate cu ISP, hardware sau software.....	106
3.4 DESFĂȘURAREA LUCRĂRII	106
3.1 PĂCĂLIREA FIREWALL/IDSURILOR ȘI ASCUNDEREA IDENTITĂȚII	107
L4 PROXY SERVER.....	111
4.1 OBIECTIVE:	111
4.2 GENERALITĂȚI/DEFINIȚII SERVER PROXY	111
4.3 SERVER PROXY PENTRU WINDOWS.....	111
4.4 DESFĂȘURAREA LUCRĂRII	113
4.4.1 Instalare și configurare server proxy WinGate	113
4.4.2 Instalare și configurare Client proxy WinGate.....	115
4.4.3 Modurile de lucru ale Winsock Redirection Application.....	117
L5 PROXY SERVER SQUID PE SISTEM DE OPERARE LINUX.....	118

5.1	OBIECTIVE:	118
5.2	GENERALITĂȚI/DEFINIȚII SERVER PROXY	118
5.3	CONFIGURAREA SQUID PENTRU LINUX	118
5.4	DESFĂȘURAREA LUCRĂRII	122
L6	OPEN VPN	126
6.1	OBIECTIVE:	126
6.2	INTRODUCERE ÎN OPENVPN.....	126
6.3	APLICAȚIE EXPERIMENTALĂ	126
6.3.1	<i>Pe sistemul server</i>	127
6.3.2	<i>Pe sistemul client</i>	128