



UNIVERSITA` DI PISA

FACOLTA` DI INGEGNERIA

CORSO DI LAUREA IN INGEGNERIA DELLE
TELECOMUNICAZIONI

Tesi di laurea:

**Tecniche di Classificazione
di traffico IPsec basate su SVM.**

Relatore: Prof. Michele Pagano

Relatore: Prof. Stefano Giordano

Relatore: Ing. Christian Callegari

Relatore: Ing. Teresa Pepe

Candidato: Giulia Orsini

ANNO ACCADEMICO 2009/2010

Indice

Elenco delle figure	
Elenco delle tabelle	
Introduzione	i
1 IPSEC.	1
1.1 Servizi offerti da IPsec	2
1.2 Alcune applicazioni di IPsec	3
1.3 Security Association e Security Association Database	3
1.3.1 Struttura delle SA contenute nel SAD	5
1.4 Security Policy e Security Policy Database.	7
1.4.1 Struttura delle SP	7
1.5 Invio e Ricezione di un messaggio.	9
1.6 Modalità Trasporto e Modalità Tunnel	11
1.7 I protocolli di IPsec	13
1.7.1 Il protocollo Authentication Header (AH)	13
1.7.1.1 AH in modalità Trasporto e in modalità Tunnel	16
1.7.1.2 Servizio Anti-Replay di AH	19
1.7.1.3 AH e NAT	21
1.7.2 Il protocollo Encapsulating Security Payload (ESP)	21
1.7.2.1 ESP in modalità Trasporto e in modalità Tunnel	24
1.7.3 Il protocollo Internet Key Exchange (IKE)	27

1.7.3.1 Fase 1 del Protocollo IKE	27
1.7.3.2 Fase 2 del Protocollo IKE	30
2 Support Vector Machines (SVMs)	31
2.1 Classificazione binaria tramite Support Vector Machines	33
2.1.1 Classificatore lineare su dati linearmente separabili	34
2.1.2 Classificatore lineare su dati non linearmente separabili	40
2.1.3 Classificatore non lineare	43
2.2 SVM Multiclass	51
3 Classificazione di Traffico IPsec	52
3.1 Creazione dello scenario previsto e instaurazione del Tunnel IPsec	53
3.2 Marcatura dei pacchetti e raccolta delle tracce	58
3.3 Il classificatore LIBSVM	60
3.3.1 Normalizzazione dei dati	61
3.3.2 Cross-Validazione e Grid-Search	62
3.4 Scrittura dei file di Training e di Testing per il classificatore LIBSVM.	63

4 Risultati Sperimentali	68
4.1 Risultati della classificazione delle tracce IPsec	70
4.1.1 Classificazione di 4 protocolli applicativi utilizzando 2 attributi.	71
4.1.2 Classificazione di 4 protocolli applicativi utilizzando 3 attributi, e confronto con i risultati ottenuti utilizzando 2 attributi.	83
4.1.3 Classificazione di 3 protocolli applicativi.	92
4.2 Risultati della classificazione delle tracce IPsec fornite dalla facoltà di Ingegneria delle Telecomunicazioni dell'Università La Sapienza di Roma.	103
4.2.1 Classificazione di 4 protocolli applicativi utilizzando 2 attributi.	103
4.2.2 Classificazione di 4 protocolli applicativi utilizzando 3 attributi, e confronto con i risultati ottenuti utilizzando 2 attributi.	114
4.2.3 Classificazione di 3 protocolli applicativi.	123
Conclusioni	133
Bibliografia	

Elenco delle figure

Fig. 1.1 Connessione logica unidirezionale tra due host.	4
Fig. 1.2 SAD che contiene le SAs.	5
Fig. 1.3 SPD che contiene le SPs.	8
Fig. 1.4 Processing dei pacchetti inviati.	10
Fig. 1.5 Processing dei pacchetti ricevuti.	11
Fig. 1.6 La modalità Trasporto protegge i livelli superiori ma non l'header IP.	12
Fig. 1.7 La modalità Tunnel protegge l'intero pacchetto originale.	13
Fig. 1.8 Struttura di AH.	14
Fig. 1.9 Header IP, in verde i campi immutabili, in giallo quelli predicibili al destinatario e in rosso i campi settati a 0.	16
Fig. 1.10 IPsec con AH in modalità Trasporto.	17
Fig. 1.11 IPsec con AH in modalità Tunnel.	18
Fig. 1.12 AH in IPv6.	19
Fig. 1.13 Meccanismo di tipo Sliding Window implementato al ricevitore per difendersi da attacchi Replay.	20
Fig. 1.14 Formato di ESP.	22

Fig. 1.15 ESP in IPv6.	24
Fig. 1.16 IPsec con ESP in modalità Trasporto.	25
Fig. 1.17 IPsec con ESP in modalità Tunnel.	26
Fig. 1.18 Messaggi nella prima fase di IKE in modalità Main.	28
Fig. 1.19 Messaggi nella prima fase di IKE in modalità Aggressive.	29
Fig. 1.20 Messaggi scambiati durante la fase 2 del protocollo IKE in modalità Quick.	30
Fig. 2.1 Dati linearmente separabili	36
Fig. 2.2 Esempi di margine piccolo (a) e margine grande (b)	37
Fig. 2.3 Piano separatore per un insieme di punti non linearmente separabili.	41
Fig. 2.4 Trasformazione dei dati non linearmente separabili in linearmente separabili, per mezzo della funzione Φ .	43
Fig. 2.5 Esempio di trasformazione in dati linearmente separabili.	44
Fig. 2.6 Matrice Kernel	46
Fig. 3.1 Scenario creato per la raccolta delle tracce IPsec.	53
Fig. 3.2 Sintassi del file etc/racoon/psk.txt per PC2.	54
Fig. 3.3 Sintassi del file etc/racoon/psk.txt per PC3.	55
Fig. 3.4 File di configurazione etc/racoon/racoon.conf di PC2.	56

Fig. 3.5 File di configurazione etc/racoon/racoon.conf di PC3.	56
Fig. 3.6 File /etc/ipsec.conf che specifica le security polizie del PC2.	57
Fig. 3.7 File /etc/ipsec.conf che specifica le security polizie del PC3.	57
Fig. 3.8 Esempio di pacchetti raccolti tramite Wireshark.	64
Fig. 3.9 Esempio di file di Training con 3 attributi.	66

Elenco delle Tabelle

Tab.4.1a Confronto classificazione con file di Training con N=1000 pacchetti e N=5000 pacchetti per il protocollo Http.	72
Tab.4.1b Confronto classificazione con file di Training con N=1000 pacchetti e N=5000 pacchetti per il protocollo Ftp.	73
Tab.4.1c Confronto classificazione con file di Training con N=1000 pacchetti e N=5000 pacchetti per il protocollo Pop3.	74
Tab.4.1d Confronto classificazione con file di Training con N=1000 pacchetti e N=5000 pacchetti per il protocollo Bittorrent.	75
Tab. 4.2 Risultati Test 3, con evidenziazione dei protocolli applicativi assegnati incorrettamente.	76
Tab. 4.3 Risultati Test 2, con evidenziazione dei protocolli applicativi assegnati incorrettamente.	76
Tab. 4.4 Risultati Test 4, con evidenziazione dei protocolli applicativi assegnati incorrettamente.	77
Tab. 4.5a Confronto classificazione del protocollo Http, con file di Training con N=1000 pacchetti e n=250 pacchetti per ogni protocollo applicativo.	78

Tab. 4.5b Confronto classificazione del protocollo Ftp, con file di Training con N=1000 pacchetti e n=250 pacchetti per ogni protocollo applicativo.	79
Tab. 4.5c Confronto classificazione del protocollo Pop3, con file di Training con N=1000 pacchetti e n=250 pacchetti per ogni protocollo applicativo.	80
Tab. 4.5d Confronto classificazione del protocollo Bittorrent, con file di Training con N=1000 pacchetti e n=250 pacchetti per ogni protocollo applicativo.	81
Tab. 4.6 Risultati Test 3, con evidenziazione dei protocolli applicativi assegnati incorrettamente.	82
Tab. 4.7 Risultati Test 2, con evidenziazione dei protocolli applicativi assegnati incorrettamente.	82
Tab. 4.8a Classificazione del protocollo Http con 2 e 3 attributi e classificazione dei pacchetti della direzione client-server.	84
Tab. 4.8b Classificazione del protocollo Ftp con 2 e 3 attributi e classificazione dei pacchetti della direzione client-server.	85
Tab. 4.8c Classificazione del protocollo Pop3 con 2 e 3 attributi e classificazione dei pacchetti della direzione client-server.	86
Tab. 4.8d Classificazione del protocollo Bittorrent con 2 e 3 attributi e classificazione dei pacchetti della direzione client-server.	87

Tab. 4.9a Classificazione del protocollo Http con 2 e 3 attributi e classificazione dei pacchetti della direzione client-server, con file di Training con 250 pacchetti per ogni protocollo applicativo.	88
Tab. 4.9b Classificazione del protocollo Ftp con 2 e 3 attributi e classificazione dei pacchetti della direzione client-server, con file di Training con 250 pacchetti per ogni protocollo applicativo.	89
Tab. 4.9c Classificazione del protocollo Pop3 con 2 e 3 attributi e classificazione dei pacchetti della direzione client-server, con file di Training con 250 pacchetti per ogni protocollo applicativo.	90
Tab. 4.9d Classificazione del protocollo Bittorrent con 2 e 3 attributi e classificazione dei pacchetti della direzione client-server, con file di Training con 250 pacchetti per ogni protocollo applicativo.	91
Tab. 4.10a Classificazione del protocollo Http con altri 2 protocolli applicativi.	92
Tab. 4.10b Classificazione del protocollo Ftp con altri 2 protocolli applicativi.	93
Tab. 4.10c Classificazione del protocollo Pop3 con altri 2 protocolli applicativi.	94
Tab. 4.10d Classificazione del protocollo Bittorrent con altri 2 protocolli applicativi.	95
Tab. 4.11 Risultati Test 3, con evidenziazione dei protocolli applicativi assegnati incorrettamente, escludendo il protocollo Http.	96

Tab. 4.12 Risultati Test 2, con evidenziazione dei protocolli applicativi assegnati incorrettamente, escludendo il protocollo Http.	97
Tab. 4.13 Risultati Test 4, con evidenziazione dei protocolli applicativi assegnati incorrettamente, escludendo il protocollo Http.	98
Tab. 4.14a Classificazione del protocollo Http con altri 2 protocolli applicativi.	99
Tab. 4.14b Classificazione del protocollo Ftp con altri 2 protocolli applicativi.	100
Tab. 4.14c Classificazione del protocollo Pop3 con altri 2 protocolli applicativi.	101
Tab. 4.14d Classificazione del protocollo Bittorrent con altri 2 protocolli applicativi.	102
Tab.4.15a Confronto classificazione con file di Training con N=1000 pacchetti e N=5000 pacchetti per il protocollo Http.	104
Tab.4.15b Confronto classificazione con file di Training con N=1000 pacchetti e N=5000 pacchetti per il protocollo Ftp.	105
Tab.4.15c Confronto classificazione con file di Training con N=1000 pacchetti e N=5000 pacchetti per il protocollo Pop3.	106
Tab.4.15d Confronto classificazione con file di Training con N=1000 pacchetti e N=5000 pacchetti per il protocollo Http.	107

Tab. 4.16 Risultati Test 3, con evidenziazione dei protocolli applicativi assegnati incorrettamente.	108
Tab. 4.17 Risultati Test 4, con evidenziazione dei protocolli applicativi assegnati incorrettamente.	108
Tab. 4.18a Confronto classificazione del protocollo Http, con file di Training con N=1000 pacchetti e n=250 pacchetti per ogni protocollo applicativo.	109
Tab. 4.18b Confronto classificazione del protocollo Ftp, con file di Training con N=1000 pacchetti e n=250 pacchetti per ogni protocollo applicativo.	110
Tab. 4.18c Confronto classificazione del protocollo Pop3, con file di Training con N=1000 pacchetti e n=250 pacchetti per ogni protocollo applicativo.	111
Tab. 4.18d Confronto classificazione del protocollo VoIP con codifica G.726-16, con file di Training con N=1000 pacchetti e n=250 pacchetti per ogni protocollo applicativo.	112
Tab. 4.19 Risultati Test 3, con evidenziazione dei protocolli applicativi assegnati incorrettamente.	113
Tab. 4.20 Risultati Test 2, con evidenziazione dei protocolli applicativi assegnati incorrettamente.	113

Tab. 4.21a Classificazione del protocollo Http con 2 e 3 attributi e classificazione dei pacchetti nella direzione client-server.	115
Tab. 4.21b Classificazione del protocollo Ftp con 2 e 3 attributi e classificazione dei pacchetti nella direzione client-server.	116
Tab. 4.21c Classificazione del protocollo Pop3 con 2 e 3 attributi e classificazione dei pacchetti nella direzione client-server.	117
Tab. 4.21d Classificazione del protocollo VoIP con codifica G.726-16 con 2 e 3 attributi e classificazione dei pacchetti nella direzione client-server.	118
Tab. 4.22a Classificazione del protocollo Http con 2 e 3 attributi e classificazione dei pacchetti nella direzione client-server, con file di Training con 250 pacchetti per ogni protocollo applicativo.	119
Tab. 4.22b Classificazione del protocollo Ftp con 2 e 3 attributi e classificazione dei pacchetti nella direzione client-server, con file di Training con 250 pacchetti per ogni protocollo applicativo.	120
Tab. 4.22c Classificazione del protocollo Pop3 con 2 e 3 attributi e classificazione dei pacchetti nella direzione client-server, con file di Training con 250 pacchetti per ogni protocollo applicativo.	121
Tab. 4.22d Classificazione del protocollo VoIP con codifica G.726-16 con 2 e 3 attributi e classificazione dei pacchetti nella direzione client-server, con file di Training con 250 pacchetti per ogni protocollo applicativo.	122

Tab. 4.23a Classificazione del protocollo Http con altri 2 protocolli applicativi.	123
Tab. 4.23b Classificazione del protocollo Ftp con altri 2 protocolli applicativi.	124
Tab. 4.23c Classificazione del protocollo Pop3 con altri 2 protocolli applicativi.	125
Tab. 4.23d Classificazione del protocollo VoIP con codifica G.726-16 con altri 2 protocolli applicativi.	126
Tab. 4.24 Risultati Test 3, con evidenziazione dei protocolli applicativi assegnati incorrettamente, escludendo il protocollo VoIP.	127
Tab. 4.25 Risultati Test 4, con evidenziazione dei protocolli applicativi assegnati incorrettamente, escludendo il protocollo Ftp.	127
Tab. 4.26a Classificazione del protocollo Http con altri 2 protocolli applicativi.	129
Tab. 4.26b Classificazione del protocollo Ftp con altri 2 protocolli applicativi.	130
Tab. 4.26c Classificazione del protocollo Pop3 con altri 2 protocolli applicativi.	131
Tab. 4.26d Classificazione del protocollo VoIP con altri 2 protocolli applicativi.	132