Sicurezza IP

IP Security Overview

- 1994 **RFC1636**, "Security in the Internet Architecture"
- Necessità di:
 - Un'infrastruttura di rete sicura da monitoraggio non autorizzato
 - Controllare traffic di rete
- Comunicazioni end-to-end sicure, usando _{Sicurezza IP} crittografia e autenticazione

2

IP Security Overview

- CERT most serious attacks are IP spoofing and eavesdropping/packet sniffing
- Next generation IP includes
 authentication and encryption
- IPv6

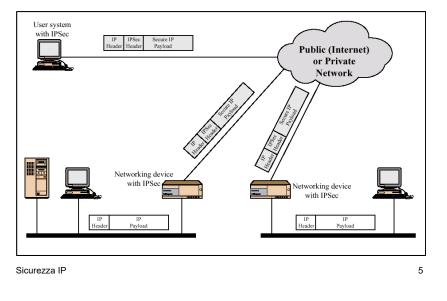
Sicurezza IP

- IPSec \subset IPv6
- Available with IPv4

Applicazioni di IPSec

- Rendere sicura
 - la connessione Internet delle organizzazioni
 - La possibilità di accedere a servizi in remoto mediante Internet
- Stabilire connettività extranet e intranet con partner
- sicurezza nell'e-commerce 4

Applicazioni di IPSec



Benefici

- Rafforzare la sicurezza per il traffico che attraversa il perimetro, assumendo che sia implementato da un firewall o un router
- Trasparente
 - Alle applicazioni
 - Agli utenti

Sicurezza IP

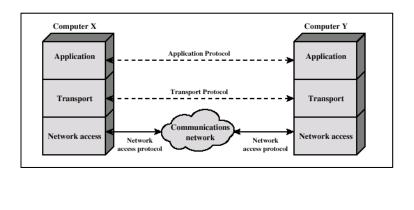
Routing & IPSec

- Requisiti:
 - Richieste di instradamento devono venire da router autorizzati
 - Richieste di redirezionamento devono venire dal router verso cui i pacchetti sono stati originariamente indirizzati
 - Prevenire distruzioni di pacchetti o invio di traffico verso direzioni non volute

Network Security

Basic Networking – Part A

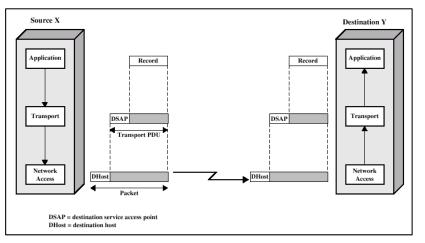
Protocols in a Simplified Architecture



Sicurezza IP

Operation of a Protocol

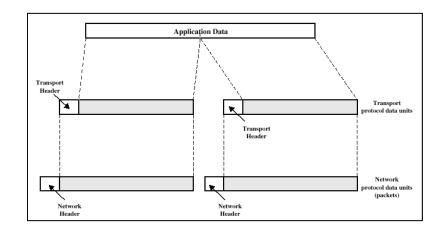
Architecture



Sicurezza IP

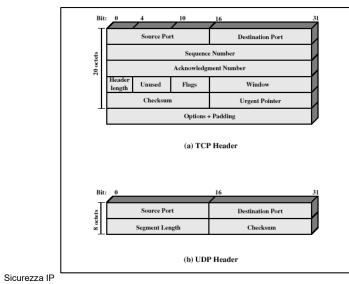
9

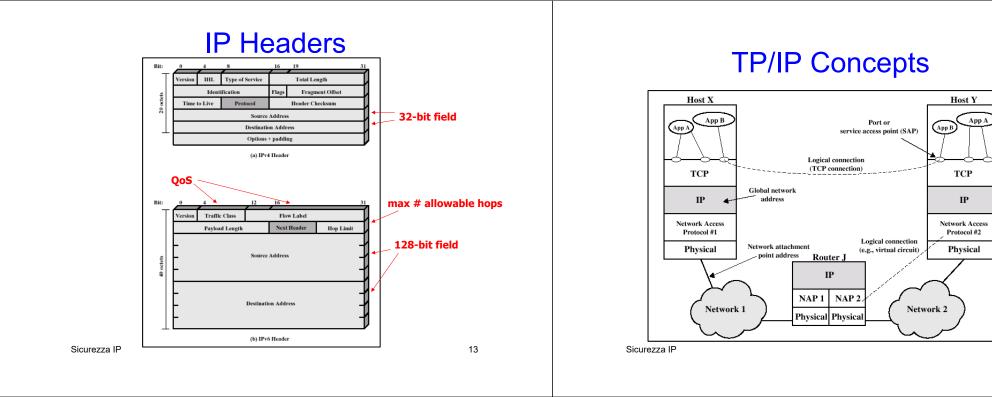
Protocol Data Units



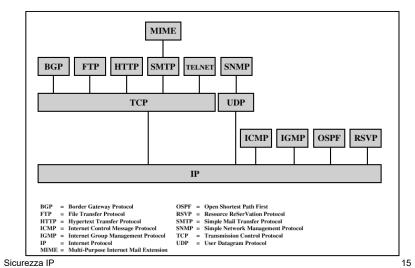
Sicurezza IP

TCP and UDP Headers

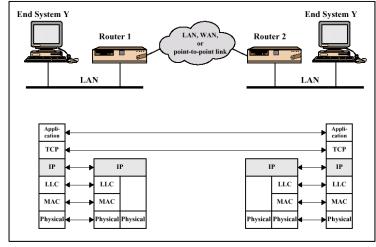




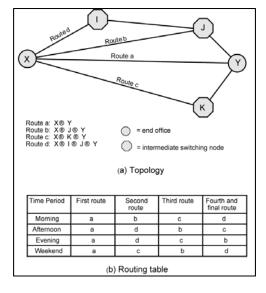
Some TCP/IP Protocols



Configuration of TCP/IP



Alternate Routing Diagram





Network Security

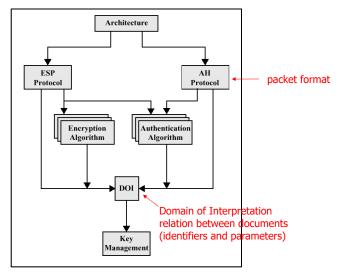
IP Security – Part 1

Sicurezza IP

IPSec Documents

- November 1998
 - RFC 2401 Overview
 - RFC 2402 Packet Authentication Extension
 - RFC 2406 Packet Encryption Extension
 - RFC 2408 Key Management Capabilities
- Implemented as extension headers that follow the main header:
 - Authentication Header (AH)
 - Encapsulating Security Payload Header (ESP)

IPSec Documents



Sicurezza IP

17

IPSec: Servizi

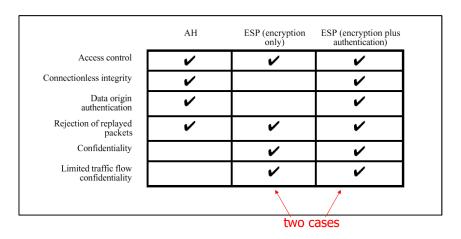
- Fornisce servizi di sicurezza al livello di Internet protocol
- Permette al sistema di:
 - Selezionare i protocolli di sicurezza opportuni
 - Determinare gli algoritmi di sicurezza da usare
 - Definire le chiavi necessarie

21

Servizi IPSec – 2 Protocolli

- Authentication protocol designated by the authentication header (AH)
- Encryption/Authentication protocol designated by the format of the packet, Encapsulating Security Payload (ESP); it is a mechanism for providing *integrity* and *confidentiality* to IP datagrams
- AH and ESP are vehicles for access

IPSec Services



Associations per la IPSec

Concetto chiave:

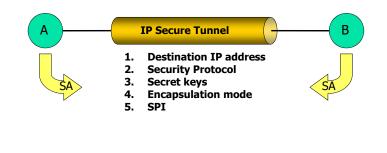
- Security Association (SA) is a oneway relationship between a sender and a receiver that defines the security services that are provided to a user
- I requisiti sono specificati in 2 database: security policy database (SPD) e security association database (SAD)

Security Associations

Uniquely identified by:

- Destination IP address address of the destination endpoint of the SA (end user system or firewall/router)
- Security protocol whether association is AH or ESP. Defines key size, lifetime and crypto algorithms (transforms)
- Security parameter index (SPI) bit string that provides the receiving device with info on how to process the incoming traffic

Security Associations



Sicurezza IP	25	Sicurezza IP

Security Associations

- SA è unidirezionale
- Definisce le operazioni che occorrono solo in una direzione
- La bidirzionalità richiede una coppia di SA (e.g., secure tunnel)
- Two SAs use the same metacharacteristics but employ different keys

Security Association Database

- Each IPSec implementation has a Security Association Database (SAD)
- SAD defines the parameters association (SPI) with each SA
- SAD stores pairs of SA, since SAs are unidirectional

Sicurezza IP

Security Association Database

- Sequence number counter
- Sequence counter overflow
- Anti-replay window
- . AH information
- ESP information
- Lifetime of this SA
- · IPSec protocol mode tunnel, transport, wildcard

Siculezath MTU

29

Security Policy Database

- Provides considerable flexibility in way IPSec services are applied to IP traffic
- Can discriminate between traffic that is afforded IPSec protection and traffic allowed to bypass IPSec
- The Security Policy Database (SPD) is the means by which IP traffic is related to specific SAs

Sicurezza II	Ρ
--------------	---

Security Policy Database

- Each entry defines a subset of IP traffic and points to an SA for that traffic
- These selectors are used to filter outgoing traffic in order to map it into a particular SA

Security Policy Database

- **Destination IP address**
- Source IP address
- User ID
- Data sensitivity level secret or unclassified
- Transport layer protocol
- . IPSec protocol AH or ESP or AH/ESP
- Source and destination ports
- · IPv6 class
- . IPv6 flow label
- . IPv4 type of service (TOS)

Security Policy Database

Outbound processing of packet:

- 1)Compare fields in the packet to find a matching SPD entry
- 2)Determine the SA and its associated SPI
- 3)Do the required IPSec processing

Sicurezza IP

33

Transport and Tunnel Modes

• SA supports two modes:

Transport – protection for the upper layer protocols

Tunnel – protection for the entire IP packet

Transport Mode

- Protection extends to the payload of an IP packet
- Primarily for upper layer protocols TCP, UDP, ICMP
- Mostly used for end-to-end communication
- For AH or ESP the payload is the data following the IP header (IPv4) and IPv6 extensions
- Encrypts and/or authenticates the payload, but *not the IP header*

Tunnel Mode

- Protection for the entire packet
- Add new *outer* IP packet with a new outer header
- AH or ESP fields are added to the IP packet and entire packet is treated as payload of the outer packet
- Packet travels through a *tunnel* from point to point in the network

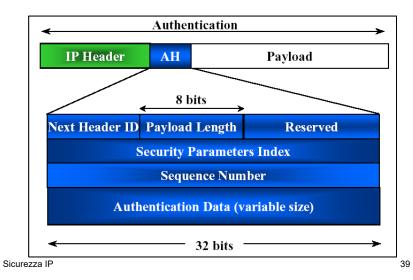
Tunnel and Transport Mode

	Transport Mode SA	Tunnel Mode SA
АН	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	Encrypts inner IP packet.
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.	Encrypts inner IP packet. Authenticates inner IP packet.

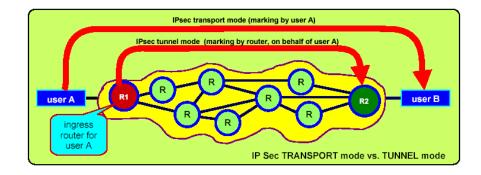
Sicurezza IP

37

Authentication Header



Transport vs Tunnel Mode



Sicurezza IP

38

Authentication Header

- Provides support for data integrity and authentication of IP packets
- Undetected modification in transit is impossible
- Authenticate the user or application and filters traffic accordingly
- Prevents address spoofing attacks
- Guards against replay attacks
- Based on the use of a message authentication
 code (MAC) so two parties must share a key
 sicurezza IP

IPSec Authentication Header

Bit:	0	8	16	31
[Next Header	Payload Length	RESERVED	
		Security Parame	eters Index (SPI)	
		Sequence	Number	
	_	Authentication	Data (variable)	

Sicurezza IP

Authentication Header

- Next header type of header following
- Payload length length of AH
- Reserved future use
- Security Parameters Index idents SA
- Sequence Number 32bit counter
- Authentication data variable field that contains the Integrity Check Value (ICV), or MAC

Sicurezza IF

42

44

Servizio Anti-Replay

- Replay Attack: Obtain a copy of authenticated packet and later transmit to the intended destination
- Mainly disrupts service
- Sequence number is designed to prevent this type of attack

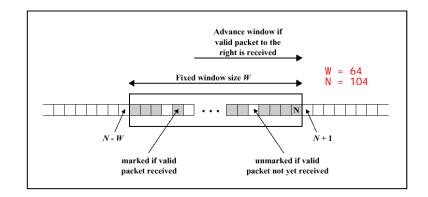
Servizio Anti-Replay

- Sender inizializza un contatore (seq num) a 0 e lo incrementa per ogni pck inviato
- Seq num < 2³²; otherwise new SA
- IP is connectionless, unreliable service
- Receiver implements window of W
- Right edge of window is highest seq

Servizio Anti-Replay

- Per ogni nuovo pck ricevuto all'interno di una window si verifica il MAC, e se autenticato viene marcato
- I pck sul lato destroy della window svolgono il check/mark & advance window verso il nuovo seq num che è il nuovo right edge
- Packet to the left, or authentication fails, discard packet, & flag event

Anti-Replay Mechanism

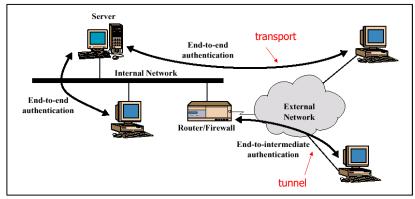


Sicurezza IP

Integrity Check Value

- Verificato grazie all'Authentication Data field
- . ICV è un Message Authentication Code (MAC)
- Consiste di una versione troncata di un codice prodotto dall'algoritmo del MAC
- HMAC value è calcolato da solo I primi 96 bit
- MAC è calcolato a partire da un campo fisso, e.g., source address in IPv4

End-to-end Authentication



Two Ways To Use IPSec Authentication Service

AH Tunnel and Transport Modes

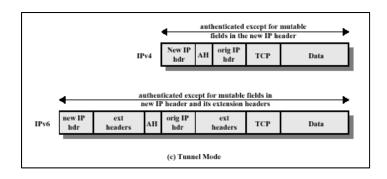
- Considerations are different for IPv4 and IPv6
- Authentication covers the entire packet
- Mutable fields are set to 0 for MAC calculation

What's a mutable field?

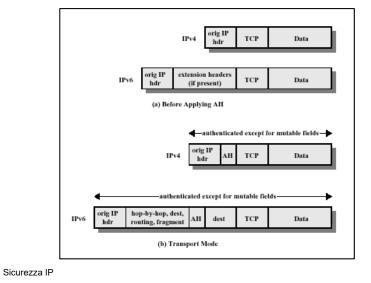
Sicurezza	IP	

49

Scope of AH Authentication



Scope of AH Authentication



Important URLs

- www.rfc-editor.org Search for RFC 1636, Security in the Internet Architecture, and other RFCs related to IPSec
- <u>http://en.wikipedia.org/wiki/IPV6</u> Great info and links related to IPv6
- <u>http://www.ipv6tf.org/</u> This portal has lots of news and info about IPv6

Important URLs

http://www.ipv6.org/

Includes introductory material, news on recent IPv6 product developments, and related links.

www.redbooks.ibm.com/pubs/pdfs/redbooks/gg243376.pdf Very good TCP/IP Tutorial from IBM Redbook Series with a good section (chap. 5) on security

Network Security

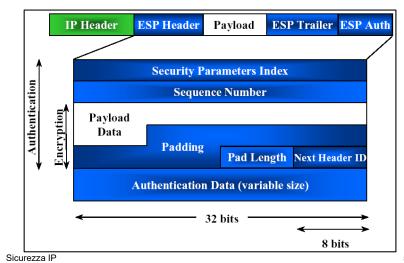
IP Security – Part 2

Sicurezza IP 53 Sicurezza IP 54

Encapsulating Security Payload

- Fornisce servizi di confidentiality
 - confidenzialità dei contenuti di un msg e limitata confidenzialità di del flusso del traffico
- ESP can also provide the same authentication services as AH

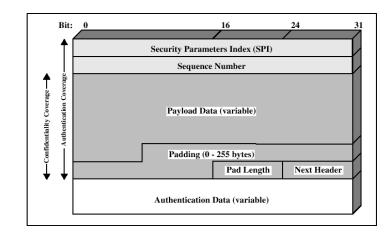
Encapsulating Security Payload



Encapsulating Security Payload

- Security Parameters Index idents SA
- Sequence Number 32bit counter
- Payload Data variable field protected by encryption
- Padding 0 to 255 bytes
- Pad Length number of bytes in preceding
- Next header type of header following
- Authentication data variable field that contains the Integrity Check Value (ICV)

IPSec ESP Format



Sicurezza IP

ESP and AH Algorithms

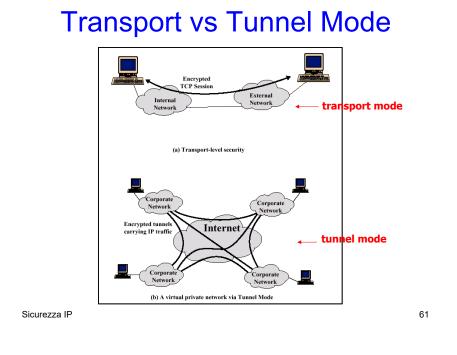
- Le implementazioni devono supportare DES in cipher block chaining (CBC) mode
- Others: 3DES, PC5, IDA, 3IDEA, CAST, Blowfish
- ESP support use of a 96bit MAC similar to AH

ESP Padding

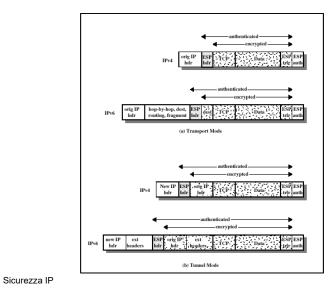
- Algorithm may require plaintext to be a multiple of some number of bytes
- Pad Length and Next Header must be right aligned
- Additional padding may be used to conceal actual length of the payload

Sicurezza IP

57



Scope of ESP Encryption



Combining SAs

- SA can implement *either* AH *or* ESP protocol, *but not both*
- Traffic flow may require separate IPSec services between hosts
- Security Association Bundle refers to a sequence of SAs
- SAs in a bundle may terminate at different end points

Combining SAs

- SAs many combine into bundles in two ways:
 - Transport adjacency applying more than one security protocol to the same IP packet without invoking tunneling; only one level of combination, no nesting
 - Iterated tunneling application of mutitiple layers of security protocols effected through IP tunneling; multiple layers of nesting

Authentication + Encryption

- Several approaches to combining authentication and confidentiality
- ESP with Authentication Option
 - First apply ESP then append the authentication data field
 - Authentication applies to ciphertext rather than plaintext

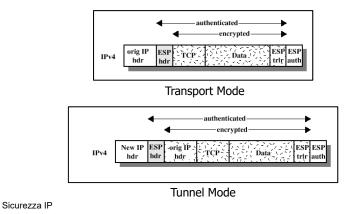
Sicurezza IP

Authentication + Encryption

- Transport Adjacency
 - Use two bundled transport SAs
 - Inner being an ESP SA; outer being an AH SA
 - Authentication covers the ESP plus the original IP header
 - Advantage: authentication covers more fields, including source and destination IP addresses

Authentication + Encryption

• ESP with Authentication Option



66

Authentication + Encryption

Transport-Tunnel Bundle

- First apply authentication, then encryption
- Authenticated data is protected and easier to store and retrieve
- Use a bundle consisting of an inner AH transport
 SA and an outer ESP tunnel SA
- Advantage: entire authenticated inner packet is encrypted and a new outer IP header is added

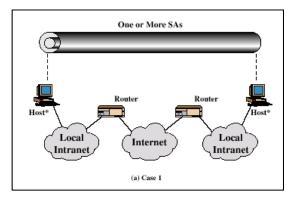
Basic Combinations

- IPSec architecture descrive 4 esempi che devono essere supportati nelle implementazioni
- Sono rappresentate le connessioni logiche e fisiche
- Ogni SA può essere sia AH che ESP
- Host-to-host SAs are either transport or Sicureztumnel, otherwise it must be tunnel mode⁶⁹

Basic Combinations – Case 1

- All security is provided between end systems that implement IPSec
- Possible combinations
 - a. AH in transport mode
 - b. ESP in transport mode
 - c. AH followed by ESP in transport mode (an AH SA inside an ESP SA)
- d. Any one of a, b, or c inside and AH or ESP in tunnel mode

Basic Combinations – Case 1

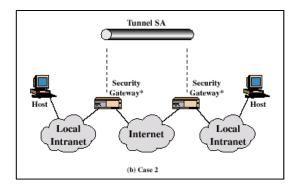


* = implements IPSec

Basic Combinations – Case 2

- Security is provided only between gateways and no hosts implement IPSec
- VPN Virtual Private Network
- Only single tunnel needed (support AH, ESP or ESP w/auth)

Basic Combinations – Case 2



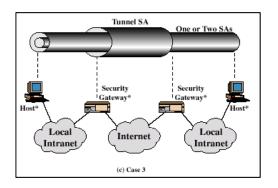
* = implements IPSec

Sicurezza IP

Basic Combinations – Case 3

- Builds on Case 2 by adding end-to-end security
- Gateway-to-gateway tunnel is ESP
- Individual hosts can implement additional IPSec services via end-to-end SAs

Basic Combinations – Case 3



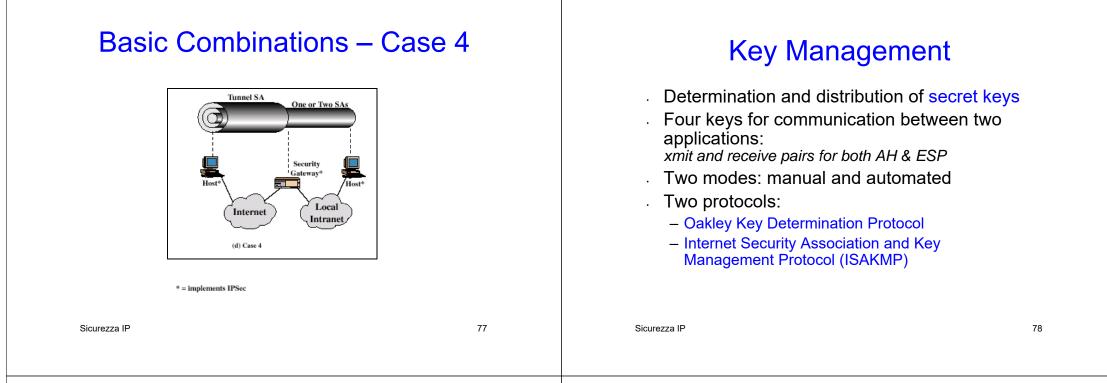
* = implements IPSec

Basic Combinations – Case 4

- Provides support for a remote host using the Internet and reaching behind a firewall
- Only tunnel mode is required between the remote host and the firewall
- One or two SAs may be used between the remote host and the local host

Sicurezza IP

73



Oakley Key Determination Protocol

- Refinement of the Diffe-Hellman key exchange algorithm
- Two users A and B agree on two global parameters: q, a large prime number and α, a primitive root of q
- Secret keys created only when needed
- Exchange requires no preexisting infrastructure
- Disadvantage: Subject to MITM attack

Features of Oakley

- Employs cookies to thwart clogging attacks
- Two parties can negotiate a group (modular exponentiation or elliptic curves)
- Uses nonces to ensure against replay attacks
- Enables the exchange of Diffie-Hellman public key values
- Authenticates the Diffie-Hellman exchange to thwart MITM attacks
 Sicurezza IP

Aggressive Oakley Key Exchange

$$\begin{split} \left[\rightarrow R: CKY_{I}, OK_{KEYX}, GRP, g^{x}, EHAO, NIDP, ID_{I}, ID_{R}, N_{I}, S_{KI}[ID_{I} \parallel ID_{R} \parallel N_{I} \parallel GRP \parallel g^{x} \parallel EHAO] \\ R \rightarrow I: CKY_{R}, CKY_{I}, OK_{KEYX}, GRP, g^{y}, EHAS, NIDP, ID_{R}, ID_{I}, N_{R}, N_{I}, S_{KR}[ID_{R} \parallel ID_{I} \parallel N_{R} \parallel N_{I} \parallel GRP \parallel g^{y} \parallel g^{x} \parallel EHAS] \\ I \rightarrow R: CKY_{I}, CKY_{R}, OK_{KEYX}, GRP, g^{x}, EHAS, NIDP, ID_{I}, ID_{R}, N_{I}, N_{R}, S_{KI}[ID_{I} \parallel ID_{R} \parallel N_{I} \parallel N_{R} \parallel GRP \parallel g^{y} \parallel g^{y} \parallel EHAS] \\ Notation: I = Initiator \\ R = Responder \\ CKY_{I}, CKY_{R} = Initiator, responder cookies \\ OK_{KEYX} = Key exchange message type \\ GRP = Name of Diffie-Hellman group for this exchange \\ g^{x}, g^{y} = Public key of initiator, responder; g^{xy} = session key from this exchange \\ EHAO, EHAS = Encryption, hash, authentication functions, offered and selected \\ NIDP = Indicates encryption is not used for remainder of this message \\ ID_{I}, ID_{R} = Identifier for initiator, responder \\ N_{I}, N_{R} = Random nonce supplied by initiator, responder for this exchange \\ S_{KI}[X], S_{KR}[X] = Indicates the signature over X using the private key (signing key) of initiator, responder \\ S_{KI}[X], S_{KR}[X] = Indicates the signature over X using the private key (signing key) of initiator, responder \\ S_{KI}[X], S_{KR}[X] = Indicates the signature over X using the private key (signing key) of initiator, responder \\ S_{KI}[X], S_{KR}[X] = Indicates the signature over X using the private key (signing key) of initiator, responder \\ S_{KI}[X], S_{KR}[X] = Indicates the signature over X using the private key (signing key) of initiator, responder \\ S_{KI}[X], S_{KR}[X] = Indicates the signature over X using the private key (signing key) of initiator, responder \\ S_{KI}[X], S_{KR}[X] = Indicates the signature over X using the private key (signing key) of initiator, responder \\ S_{KI}[X], S_{KR}[X] = Indicates the signature over X using the private key (signing key) of initiator, responder \\ S_{KI}[X], S_{KR}[X] = Indicates the signature over X using the private key (signing key) of i$$

Sicurezza IP

81

83

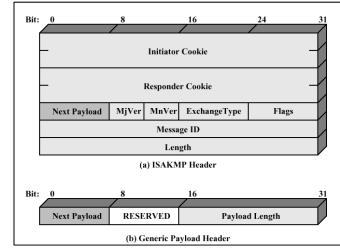
ISAKMP

- Defines procedures and packet formats to establish, negotiate, modify and delete SAs
- Defines payloads for exchanging key generation and authentication data
- Now called IKE

Sicurezza IP

82

ISAKMP Formats



ISAKMP Payload Types

Туре	Parameters	Description
Security Association (SA)	Domain of Interpretation, Situation	Used to negotiate security attributes and indicate the DOI and Situation under which negotiation is taking place.
Proposal (P)	Proposal #, Protocol-ID, SPI Size, # of Transforms, SPI	Used during SA negotiation; indicates protocol to be used and number of transforms.
Transform (T)	Transform #, Transform-ID, SA Attributes	Used during SA negotiation; indicates transform and related SA attributes.
Key Exchange (KE)	Key Exchange Data	Supports a variety of key exchange techniques.
Identification (ID)	ID Type, ID Data	Used to exchange identification information.
Certificate (CERT)	Cert Encoding, Certificate Data	Used to transport certificates and other certificate- related information.
Certificate Request (CR)	# Cert Types, Certificate Types, # Cert Auths, Certificate Authorities	Used to request certificates; indicates the types of certificates requested and the acceptable certificate authorities.
Hash (HASH)	Hash Data	Contains data generated by a hash function.
Signature (SIG)	Signature Data	Contains data generated by a digital signature function.
Nonce (NONCE)	Nonce Data	Contains a nonce.
Notification (N)	DOI, Protocol-ID, SPI Size, Notify Message Type, SPI, Notification Data	Used to transmit notification data, such as an error condition.
Delete (D)	DOI, Protocol-ID, SPI Size, # of SPIs, SPI (one or more)	Indicates an SA that is no longer valid.

ISAKMP Exchanges

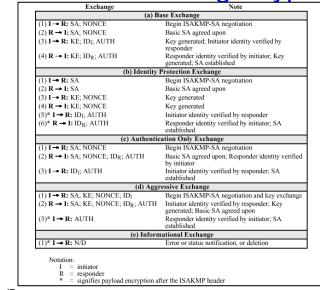
- Provides a framework for message exchange
- Payload type serves as the building blocks
- Five default exchange types specified
- SA refers to an SA payload with associated Protocol and Transform payloads

)			

Sicurezza IF

85

ISAKMP Exchange Types



Sicurezza IP

Internet Key Exchange

- IKE is now at Ver 2 defined in RFC4306, 12/05
- It works within ISAKMP framework
- Uses Oakley and Skeme protocols for authenticating keys and rapid key refreshment

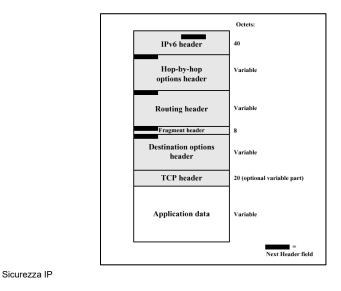
Network Security

Basic Networking – Part B

IPv6

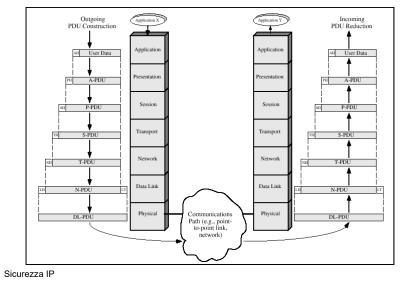
- 1995 RFC 1752 IPng
- 1998 RFC 2460 IPv6
- Functional enhancements for a mix of data streams (graphic and video)
- Driving force was address depletion 128-bit addresses
- Started in Solaris 2.8, Windows 2000

IPv6 Packet w/Extension Headers



OSI Layers Application Provides access to the OSI environment for users and also rovides distributed information services. Presentation rovides independence to the application processes from fifferences in data representation (syntax) Session Provides the control structure for communication betwee applications; establishes, manages, and terminates nnections (sessions) between cooperating application Transport rovides reliable, transparent transfer of data between end points; provides end-to-end error recovery and flow control Network Provides upper layers with independence from the data ransmission and switching technologies used to connect systems; responsible for establishing, maintaining, and erminating connection Data Link provides for the reliable transfer of information across the physical link; sends blocks (frames) with the necessary ynchronization, error control, and flow control. Physical Concerned with transmission of unstructured bit stream or physical medium; deals with the mechanical, electrical, functional, and procedural characteristics to access the ical medium. Sicurezza IP

OSI Environment



89

OSI-TCP/IP Comparison

OSI	TCP/IP	
Application		
Presentation	Application	
Session	The second se	
Transport	Transport (host-to-host)	
Network	Internet	
Data Link	Network Access	
Physical	Physical	



93

Back

Network Security

IP Security – Part 2

Sicurezza IP

94

Ethereal

- Ethereal is a free network protocol analyzer for Unix and Windows
- Packet Sniffer data can be captured "off the wire" from a live network connection
- www.ethereal.com Everything you ever wanted to know about ethereal
- <u>wiki.ethereal.com</u> This is the "User's Manual;" also has has a nice "References"
 SigurezSection

File	Edit Capt	ereal ure <u>D</u> isplay	y <u>T</u> ools		4		y bu	siness	.nytime	s.cor	n /	ACK	
No.	Time	Source		0	estinatio	in	1	Protocol	Info				
52	38.984733	VCOSTA_L	APTOP	2	05.185	.55.10	53	TCP	1126 > 80	[SYN]	Seg=1034	117 Ack=	0 Win=8192
53	39.068380	205.185.	55.163	1	COSTA_	LAPTO	>	TCP	80 > 1126				
	39.068987				05.185			TCP	1126 > 80				
	39.085030				05.185			HTTP	POST /new			tion=ne	ws_titles
	39.180178				COSTA_			HTTP	HTTP/1.1				
	39.338830				05.185			TCP	1126 > 80				
	39.758173				51.108			DNS	Standard				
	39.758227 39.804710						ny.cv.net	HTTP	Standard HTTP/1.1			00.180.2	up.iri-add
	39.804710 39.805912				COSTA_			HTTP	Continuat				
	39.805912 39.806051				05.185			TCP	1126 > 80		Sec-1041	Ins ack-	254716874
	39.806031				(COSTA			HTTP	Continuat		Seq#1043	193 ACK=	3 347 10874
	14 1417134	/		,			-		· · · · · · · · · · · · · · · · · · ·				
_	ame 55 (8)												
	Arrival T Time delt Time rela	a from pr tive to f	evious p	packet:	0.0160)43 se		\setminus	dns que	ery			
	Time delt	a from pr tive to f ber: 55	evious pa	packet:	0.0160)43 se		\	dns que	ery	_ COO	kie is	capture
220	Time delt Time rela Frame Num Packet Le 68 65 00	a from pr tive to f ber: 55 ngth: 829	evious p irst pa bytes 6f 6b	packet: cket: 3 69 65	0.0160 9.08503 3a 20	043 se 30 sec 52 4d	onds 49 44	heCook	ie: RMID	ery	_ COO	kie is	captur
220	Time delt Time rela Frame Num Packet Le 68 65 00 3d 31 38	a from pr tive to f ber: 55 ngth: 829 0 0a 43 6f 3 62 64 64	evious pa irst pa bytes 6f 6b 4 63 38	packet: cket: 3 69 65 38 33	0.0160 9.08503 3a 20 61 30)43 se 30 sec 52 4d 64 31	onds 49 44 66 36	heCook =18bddc8	ie: RMID 83a0d1f6	ery	_ COO	kie is	captur
220 230 240 250	Time delt Time rela Frame Num Packet Le 68 65 00 3d 31 38 30 3b 20 46 68 65	a from pr tive to f ber: 55 ngth: 829 0 0 43 6f 3 62 64 64 0 4e 59 54 5 7a 57 56	evious irst pa bytes 6f 6b 4 63 38 4 2d 53 5 4f 2f	69 65 38 33 3d 31 44 50	0.0160 9.08503 3a 20 61 30 30 31 6d 33	043 se 30 sec 52 4d 64 31 7a 71 6f 41	onds 49 44 66 36 33 32 54 47	heCook =18bddc8 0; NYT-S FhezwVO/	ie: RMID 83a0d1f6 =101zq32 DPm3oATG	ery	_ COO	kie is	captur
220 230 240 250 260	Time delt Time rela Frame Num Packet Le 68 65 00 3d 31 38 30 3b 20 46 68 65 2e 54 72	a from pr tive to f ber: 55 ngth: 829 0 0 43 6f 3 62 64 64 0 4e 59 56 6 7a 57 56 2 69 56 66	evious irst pa- bytes 6f 6b 4 63 38 4 2d 53 5 4f 2f 2 39 31	packet: 3 69 65 38 33 44 50 43 44	0.0160 9.08503 3a 20 61 30 30 31 6d 33 47 36	043 se 30 sec 52 4d 64 31 7a 71 6f 41 59 77	onds 49 44 66 36 33 32 54 47 57 6e	heCook =18bddc8 0; NYT-S FhezWVO/ .TriVN91	ie: RMID 83a0d1f6 =101zq32 DPm30ATG CDG6YWWN	ery	<u> </u>	kie is	captur
220 230 240 250 260 270	Time delt Time rela Frame Num Packet Le 68 65 00 3d 31 38 30 3b 20 46 68 69 2e 54 72 59 35 70	a from pr tive to f ber: 55 ngth: 829 1 0a 43 6f 3 62 64 64 0 4e 59 54 5 7a 57 56 0 50 56 68 0 30 4b 68	evious participation participa	packet: 3 69 65 38 33 3d 31 44 50 43 44 55 42	0.0160 0.08503 3a 20 61 30 30 31 6d 33 47 36 2f 49	043 se 30 sec 52 4d 64 31 7a 71 6f 41 59 77 57 39	onds 49 44 66 36 33 32 54 47 57 6e 52 76	heCook =18bddc8 0; NYT-S FhezWVO/ .TriVn91 Y5p0Kk9Z	ie: RMID 83a0dlf6 =101zq32 DPm3oATG CDG6YwWn UB/IW9RV	ery	_ COO	kie is	captur
220 230 240 250 260 270 280	Time delt Time rela Frame Num Packet Le 68 65 00 3d 31 38 30 3b 20 46 68 65 2e 54 72 59 35 72	a from pr tive to f ber: 55 ngth: 829 d 0a 43 6f d 0a 46 6f d 0a 46 6f d 0a 46 6f d 0a 6f d 0a 46 6f d 0a 66 6	evious irst par bytes 6f 6b 4 63 38 4 2d 53 5 4f 2f 2 39 31 0 39 5a 5 35 67	packet: 3 69 65 38 33 3d 31 44 50 43 44 78 4f	0.0160 0.08503 3a 20 61 30 30 31 6d 33 47 36 2f 49 73 71	043 se 30 sec 52 4d 64 31 64 31 59 77 59 77 59 77 59 77 39 2f 7a	onds 49 44 66 36 33 32 54 47 57 6e 52 76 55 34	heCook =18bddc8 0; NYT-S FhezwVO/ .TriVN91 Y5p0Kk92 ww.LoF5g	ie: RMID 83a0d1f6 =101zq32 DPm3oATG CDG6YWWn UB/IW9RV XOSq/2V4	ery	<u> </u>	kie is	captur
220 230 240 250 260 270 280 290 240	Time delt Time rela Frame Num Packet Le 68 65 00 30 3b 20 46 68 65 2e 54 72 59 35 70 59 35 70 69 5a 73 67 30 30	a from pr tive to f ber: 55 ngth: 829 1 0a 43 6f 3 62 64 64 2 64 5 74 5 7a 57 56 2 9 56 66 2 9 56 66 2 46 6f 46 5 4e 39 52 3 0 4b 6b 2 4c 6f 46 5 4e 39 52 3 32 0 52 5 32 5 32 0 52 5 32 5 32 0 52 5 32 5 32 0 52 5 32 5 32 5 32 5 32 5 32 5 32 5 32 5	evious painst pa	packet: 3 69 65 38 33 44 50 43 44 55 42 78 4f 78 4f 36 43	0.0160 3a 20 61 30 61 30 60 33 47 36 2f 49 73 71 62 44 38 30	043 sec 30 sec 52 4d 64 31 7a 71 6f 41 59 77 57 39 2f 7a 32 30	onds 49 44 66 36 33 32 54 47 57 6e 52 76 56 34 67 78 30 32	heCook =18bddc8 0; NYT-S FhezWVO/ .TriVn91 Y5p0Kk92 Ww.LoF5g iZuN9RK7	ie: RMID 83a0dlf6 =101zq32 DPm3oATG CDG6YwWn UB/IW9RV	ery	<u> </u>	kie is	captur
220 230 240 250 260 270 280 290 280 290 280	Time delt Time rela Frame Num Packet Le 68 65 00 30 31 35 30 3b 20 46 68 65 2e 54 72 59 35 70 67 30 30 67 30 30 44 32 44	a from pr tive to f ber: 55 ngth: 829 d 0a 43 6f 3 62 64 64 5 46 59 54 5 7a 57 56 2 69 56 66 5 46 39 52 5 30 40 64 5 46 39 52 5 30 30 30	evious painst pa	packet: 3 69 65 38 33 3d 31 44 50 43 44 55 42 78 4f 63 5a 3d 43 35 35	0.0160 3a 20 61 30 30 31 47 36 2f 49 73 71 62 44 38 30 33 30	043 sec 30 sec 52 4d 64 31 7a 71 6f 41 59 77 57 39 2f 7a 4e 78 32 30 31 30	onds 49 44 66 36 33 32 54 47 57 66 552 76 56 34 67 78 30 32 35 36	heCook =18bddc8 0; NYT-S FhezWVO/ .TriVN91 YSpOKk9Z WW.LoF5g iZUN9RK7 g00; RDB D2D00005	ie: RMID 83a0dlf6 =101zq32 DPm3oATG CDG6YwWn UB/TW9RV xosq/2V4 cZbDNxgx =C802002 55301056	ery *	_ COO	kie is	captur
220 230 240 250 260 270 280 290 280 290 280 290 220	Time delt Time rela Frame Num Packet Le Badet Le 30 3b 20 46 68 65 2e 54 72 59 35 70 57 57 22 69 5a 75 67 30 30 44 32 44 34 39 35	a from pr tive to f ber: 55 ngth: 829 3 62 64 64 3 62 64 64 4 59 54 5 7a 57 56 6 69 56 66 0 30 4b 68 2 69 56 66 0 30 4b 68 2 69 56 66 0 30 20 52 3 42 30 52 3 42 30 30 30 3 62 64 39 52 3 32 38 33	evious irst par bytes 6f 6b 4 63 38 4 2d 53 5 4f 2f 2 39 31 5 35 67 2 4b 37 2 44 42 3 31 30	packet: 3 69 65 38 33 3d 31 44 50 43 44 55 42 78 4f 63 5a 3d 43 35 35 31 30	0.0160 3.08503 3.20 6.1 30 3.0 31 6.1 33 4.7 36 7.3 71 6.2 44 3.8 30 3.3 30 3.1 30	043 sec 30 sec 52 4d 64 31 7a 71 66 47 57 39 27 7a 30 31 30 30 30	onds 49 44 66 36 33 32 54 47 57 6e 52 76 56 34 67 78 30 32 35 36 30 30	heCook =18bddc8 0; NYT-S FhezWVO/ .TriVn91 Y5p0Kk9Z WW.LoF5g 1ZUN9RK7 g00; RDB D2D00005 D2D00005	ie: RMID 83a0d1f6 =101zq32 DPm3oATG CDG6YwWn XDSq/zV4 cZbDNxgx =C802002 55301056 10100000	ery	<u> </u>	kie is	captur
220 230 240 250 260 270 280 290 280 290 240 220 240	Time delt Time rela Frame Num Packet Le 68 65 00 3d 31 38 30 3b 20 46 68 65 2e 54 77 59 35 70 69 5a 75 67 30 30 44 32 44 34 39 35 30 30 30	a from pr tive to f ber: 55 ngth: 829 d 0a 43 6f 3 62 64 64 0 4e 59 54 6 7a 57 56 2 69 56 66 0 30 4b 6b 5 4e 39 53 6 4e 39 53 0 3b 20 52 1 30 30 30 30 30 30 30	evious particular part	packet: 3 69 65 38 33 3d 31 44 55 42 78 45 63 45 3d 43 35 35 31 30 20 77	0.0160 3.08503 3.08503 3.08503 3.08503 3.08503 3.0850 3.08503 3.08505 3.08505 3.08505 3.08505 3.08505 3.08505 3.08505 3.08505 3.08505 3.08505 3.08505 3.08505 3.0950505 3.095050505 3.09505 3.09505 3.09505 3.09505 3.09505 3.09505	043 sec 30 sec 52 4d 64 31 6f 41 59 77 57 39 4e 78 32 30 31 30 30 30 30 468	onds 49 44 66 36 33 32 54 47 57 6e 52 76 55 34 67 78 30 32 35 36 30 32 35 36 65 72	heCook =18bddc8 0; NYT-S FhezwV0/ Y5p0Kk9Z WW.LoF5g 1ZUN9RK7 1ZUN9RK7 1ZUN9RK7 49528310 0000002;	ie: RMID 83a0d1f6 =101zq32 DPM30ATG CDG6YwWn XDSq/ZV4 cZbDNxgx =C802002 55301056 10100000 weather	ery	<u> </u>	kie is	captur
	Time delt Time rela Frame Num Packet Le 3d 31 38 30 3b 20 46 68 65 2e 54 72 59 35 70 57 57 72 69 5a 75 67 30 30 44 32 44 34 39 35 30 30 30 30	a from pr tive to f ber: 55 ngth: 829 3 62 64 64 3 62 64 64 4 59 54 5 7a 57 56 6 69 56 66 0 30 4b 68 2 69 56 66 0 30 4b 68 2 69 56 66 0 30 20 52 3 42 30 52 3 42 30 30 30 3 62 64 39 52 3 32 38 33	evious irst pa bytes 66 66 4 63 38 4 63 38 5 4f 2f 2 45 33 5 4f 2f 2 39 5a 5 30 5a 5 5a 5 5a 5 5a 5 5a 5 5a 5 5a 5 5a	packet: 3 69 65 38 33 3d 31 44 55 42 78 45 63 45 3d 43 35 35 31 30 20 77	0.0160 3.08503 3.08503 3.08503 3.08503 3.08503 3.0850 3.08503 3.08505 3.08505 3.08505 3.08505 3.08505 3.08505 3.08505 3.08505 3.08505 3.08505 3.08505 3.08505 3.0950505 3.095050505 3.09505 3.09505 3.09505 3.09505 3.09505 3.09505	043 sec 30 sec 52 4d 64 31 6f 41 59 77 57 39 4e 78 32 30 31 30 30 30 30 468	onds 49 44 66 36 33 32 54 47 57 6e 52 76 55 34 67 78 30 32 35 36 30 32 35 36 65 72	heCook =18bddc8 0; NYT-S FhezWv0/ Y5p0Kk9z ww.LoF5g izuN9Rk7 g00; RDB g00; RDB 02D00005 49528310 0000002; city=LGA	ie: RMID 83a0d1f6 =101zq32 DPm3oATG CDG6YwWn XDSq/zV4 cZbDNxgx =C802002 55301056 10100000				captur
220 230 240 250 260 220 220 220 220 220 220 220 220 22	Time delt Time rela Frame Num Packet Le 68 65 00 30 3b 20 46 68 67 29 35 70 59 35 70 59 35 70 67 30 30 44 32 44 34 39 30 63 69 74 53 49 41 44 48 46	a from pr tive to f ber: 55 ngth: 829 d 0a 43 6f 3 62 64 64 5 7a 57 56 2 30 4b 6b 2 4c 6f 46 2 40 56 56 5 4e 39 56 5 4e 39 52 5 30 30 30 30 30 30 5 32 38 33 30 30 30 30 5 4e 49 44 4 4b 4e 47	evious irst pa- bytes 6f 6b 4 63 38 4 2d 53 5 4f 2f 2 39 31 5 39 5a 5 35 67 2 4b 37 2 4b 37 2 4b 37 2 4b 37 2 44 42 3 31 30 0 32 3b 5 47 41 4 7 4 4 41	packet: 3 69 65 38 33 3d 31 44 50 43 44 55 44 78 4f 63 55 3d 43 35 35 31 30 20 77 3b 20 47 51 46 49	0.0166 0.08503 0.08503 0.08503 0.08503 0.08503 0.08503 0.08503 0.08503 0.0160 0.0160 0.0160 0.0160 0.0160 0.08503 0.08505	043 sec 52 4d 52 4d 54 31 59 77 57 39 2f 7a 30 30 74 68 59 53 59 53 59 54 59 53 59 54 59 55 59 58 59 58 50 58	onds 49 44 66 36 33 32 54 47 57 66 57 76 52 76 57 78 30 32 35 36 67 78 35 36 65 72 45 53 3d 43 48 43	heCook =18bddc8 0; NYT-5 FhezWvO/ .Trivn91 75p0Kk9z Ww.LoF5g 12un9Rk7 g00; RDB 02D00005 49528310 00000002; city=LGA SIONIDQG SIONIDQG	ie: RMID 83a0dlf6 =101zq32 DPM3oATG CDG6YwWn UB/IW9Rv x0Sq/zv4 =C802002 55301056 101.00000 weather ; ASPSES GQGRYX=C FIJPFLHC				
220 230 240 250 260 280 220 220 220 220 220 220 220 220 22	Time delt Time rela Frame Num Packet Le 68 65 00 30 3b 23 33 30 3b 22 54 30 3b 22 54 57 57 35 7 59 35 7 69 5a 7 67 30 3 44 32 44 34 39 33 30 30 32 53 49 44 44 84 84 45 44 44	a from pr tive to f ber: 55 ngth: 829 362 64 64 574 57 56 66 930 264 54 56 66 930 45 64 64 574 57 56 66 930 45 64 64 54 63 952 52 300 30 30 30 30 30 30 30 130 30 30 30 142 44 44 44	evious irst pa- bytes 6f 6b 463 38 463 38 47 42 39 31 30 30 35 33 5 67 2 44 42 30 30 32 3b 31 30 32 3b 31 47 44 41 3 4f 041	packet: 3 69 65 38 33 3d 31 44 50 43 44 55 42 78 42 78 42 63 5a 3d 43 35 35 54 63 5a 31 30 20 77 3b 20 47 51 46 49 0a 04	0.0166 3.0850 3.0850 3.0850 3.031 3.031 3.031 3.031 3.031 3.033 4.7552 4.433 3.030 3.033 4.7552 4.433 3.030 4.7552 4.433 3.00 4.7552 4.433 3.00 4.7552 4.433 3.00 4.7552 4.43552 4.7555 4.7552 4.75555 4.75555 4.75555 4.75555 4.75555 4.75555 4.75555 4.75555 4.755555 4.755555 4.7555555 4.7555555 4.7555555555555555555555555555555555555	043 sec 52 4d 52 4d 54 31 7a 71 557 7a 42 30 30 30 30 30 30 30 59 58 46 4c 56 64	onds 49 44 66 36 33 32 54 47 55 76 55 76 55 76 56 34 30 32 35 36 778 30 32 35 36 778 30 32 35 36 778 30 30 65 72 34 43 48 43 48 43 465 3d	heCook =18bddc8 0; NYT-5 Fhezwx0/ .TriVn91 Y5p0kk9z Ww.LoF5g izuN9kK7 g00; RDB D200005 21200005 49528310 0000002; city=LGA SIONIDQG NHNKNGDA EDKADC0.	ie: RMID 83a0d1f6 =101zq32 DFM30ATG CDG6YWWN UB/IW9RV x0Sq/2V4 cZbDNxgx =C802002 55301056 101.00000 weather ; ASPSES GQGRYX=C FIJPFLHC mode=		<u> </u>		
220 230 240 250 270 220 220 220 220 220 220 220 220 22	Time delt Time rela Frame Num Packet Le 68 65 00 3 d 31 33 3 3b 22 54 46 68 67 25 35 72 67 30 34 43 32 43 69 5a 77 57 57 22 69 5a 77 67 30 34 44 32 44 34 39 33 63 69 74 53 49 44 44 45 44 44 45 44 44 66 66 57	a from pr tive to f ber: 55 ngth: 829 10 a 43 6f 86 8 62 64 64 9 45 95 7 55 7 a 57 55 2 69 56 66 2 30 4b 6b 2 46 39 57 55 3 42 93 26 3 44 39 52 3 3 20 52 3 43 20 52 3 44 39 42 4 44 44 5 41 44 43 5 73 26 66	evious irst particles bytes 6f 6b 4 63 38 4 2d 53 5 4f 2f 5 39 5a 7 30 35 8 31 30 8 32 44 4 44 7 44 4 41 6 46 74 7 44 41 6 46 74 74 7 44 41 7 46 74 74 7 44 74 74 74 74 74 74 74 74 74 74 74 74	packet: 3 69 65 38 33 3d 31 44 50 44 50 43 44 57 8 47 63 5a 3d 43 3d 35 31 30 47 51 20 77 3b 20 47 51 00 69 69 69 69 69 69 69 69 69 69	0.0166 3.08503 3.08503 3.1 3.2 3.2 3.3 3.3 3.3 3.3 3.3 3.3	043 sec 52 4d 52 4d 54 31 55 71 55 73 46 31 76 41 59 77 57 73 30 30 30 30 50 53 50 53 546 66 546 67 57 72 58 53 59 53 59 53 50 53 51 53 51 53 53 53 53 53 53 53 53 53 53 53 54 54 54 55 55 53 55 55 55 53 55 53 55 55 55 53 55 55 55 53 55 55 55 55	onds 49 44 66 36 33 32 54 47 55 76 55 76 55 76 56 34 30 32 35 36 778 30 32 35 36 778 30 32 35 36 778 30 30 65 72 34 43 48 43 48 43 465 3d	heCook =18bddc8 0; NYT-5 Fhezwvo/.TriVn91 Y5p0kN92 WW.LOF5g 12uN9Rk7 g00; RoB D2000005 49528310 0000002; city=LGA SIONIDQG NHNKNGDA EDKADCO. news&act	ie: RMID 83a0dlf6 =101zq32 DPM3oATG CDG6YwWn XOSq/ZV4 cZbDNXgx =C802002 55301056 10100000 weather ; ASPSES GQGRYX=C FIJPFLHC mode ion=quot				
220 230 240 250 260 220 220 220 220 220 220 220 220 22	Time delt Time rela Frame Num Packet Le 68 65 00 3 d 31 33 3 3b 22 54 46 68 67 25 35 72 67 30 34 43 32 43 69 5a 77 57 57 22 69 5a 77 67 30 34 44 32 44 34 39 33 63 69 74 53 49 44 44 45 44 44 45 44 44 66 66 57	a from pr tive to f ber: 55 ngth: 829 362 64 64 574 57 56 66 930 264 54 56 546 59 54 574 57 56 66 930 45 64 64 546 39 52 300 30 30 30 30 30 30 30 130 30 30 30 130 30 30 30 142 44 44 44	evious irst particles bytes 6f 6b 4 63 38 4 2d 53 5 4f 2f 5 39 5a 7 30 35 8 31 30 8 32 44 4 44 7 44 4 41 6 46 74 7 44 41 6 46 74 74 7 44 41 7 46 74 74 7 44 74 74 74 74 74 74 74 74 74 74 74 74	packet: 3 69 65 38 33 3d 31 44 50 43 44 55 42 78 42 78 42 63 5a 3d 43 35 35 54 63 5a 31 30 20 77 3b 20 47 51 46 49 0a 04	0.0166 3.08503 3.08503 3.1 3.2 3.2 3.3 3.3 3.3 3.3 3.3 3.3	043 sec 52 4d 52 4d 54 31 55 71 55 73 46 31 76 41 59 77 57 73 30 30 30 30 50 53 50 53 546 66 546 67 57 72 58 53 59 53 59 53 50 53 51 53 51 53 53 53 53 53 53 53 53 53 53 53 54 54 54 55 55 53 55 55 55 53 55 53 55 55 55 53 55 55 55 53 55 55 55 55	onds 49 44 66 36 33 32 54 47 55 76 55 76 55 76 56 34 30 32 35 36 778 30 32 35 36 778 30 32 35 36 778 30 30 65 72 34 43 48 43 48 43 465 3d	heCook =18bddc8 0; NYT-5 Fhezwx0/ .TriVn91 Y5p0kk9z Ww.LoF5g izuN9kK7 g00; RDB D200005 21200005 49528310 0000002; city=LGA SIONIDQG NHNKNGDA EDKADC0.	ie: RMID 83a0dlf6 =101zq32 DPM3oATG CDG6YwWn XOSq/ZV4 cZbDNXgx =C802002 55301056 10100000 weather ; ASPSES GQGRYX=C FIJPFLHC mode ion=quot				

Ethereal Etiquette

- Be careful when and where you use this tool
- It makes people nervous
- Use prudence with the information you collect
- When in doubt, seek permission!

97

Other Sniffing Tools

- <u>Ettercap</u> is an open source software tool for computer network protocol analysis and security cracking. It can be used to intercept traffic on a network segment, capture passwords, and conduct manin-the-middle attacks against a number of common protocols.
- <u>dSniff</u> is a packet sniffer and set of traffic analysis tools. Unlike tcpdump and other low-level packet sniffers, dSniff also includes tools that decode information (passwords, most infamously) sent across the network, rather than simply capturing and printing the raw data, as do generic sniffers like Ethereal and tcpdump.
- <u>AiroPeek</u> was the first Wi-Fi (IEEE 802.11) packet analyzer, or packet sniffer, that provides network engineers with a view of the data traversing a Wireless LAN network. AiroPeek was created in 2001 and its interface was based closely on <u>EtherPeek</u>, another product from <u>WildPackets</u>, Inc. They also have some "free" utilities.
 Sicurezza IP 98

Important URLs

www.insecure.org/tools.html

Site has the top 50 security tools

- <u>Nmap</u> is a free software port scanner. It is used to evaluate the security of computers, and to discover services or servers on a computer network.
- <u>EtherApe</u> is a graphical network monitor for Unix.
 Featuring link layer, ip and TCP modes, it displays network activity graphically. Hosts and links change in size with traffic. Color coded protocols display.