Computer & Information Security (3-721-460-1)

Denial of Service Attack

Dept. of Software and Information Systems Engineering, Ben-Gurion University

Prof. Yuval Elovici, Dr. Asaf Shabtai
{elovici, shabtaia}@bgu.ac.il

Spring, 2019

Denial-Of-Service (DoS) Attack

"an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space."

(NIST Computer Security Incident Handling Guide)

Denial-of-Service (DoS)

- Exhaustion vs. disruption
- network bandwidth
  - capacity of the network links connecting a server to the Internet
  - for most organizations this is their connection to their ISP
  - Consuming network bandwidth with large volume of generated traffic
- system resources
  - aims to overload or crash the network handling software (e.g. protocol)
  - specific packets are sent and consume the limited resources available
    - SYN Spoofing attack - Table of TCP connections on the server
- application resources
  - involves a number of valid requests, each of which consumes significant resources, thus limiting the ability of the server to respond to requests from other users
    - CyberSlam – large & costly queries - severely load the Web-server's DB

Classic Denial of Service Attacks

- can use simple flooding ping command
- attacker generates higher volume of traffic from higher capacity network connection to lower capacity network connection which cannot handle these volumes of traffic
- cause loss of traffic
- source of the attack is clearly identified unless a spoofed address is used

Internet Control Message Protocol (ICMP)

- An error reporting and diagnostic utility
- Used by routers, intermediary devices, or hosts to communicate updates or error information to other routers, or hosts
- ICMP message contains three fields:
  - TYPE - identifies the ICMP message
  - CODE - further information about the associated TYPE field
  - CHECKSUM - a method for determining the integrity of the message

Message types:

0: Echo replay
1-2: Unassigned
3: Destination unreachable
4: Source quench
5: Redirected
7: Unassigned
8: Echo Request
11: Time exceeded
13: Timestamp Request
14: Timestamp reply
15: Information request
16: Information replay

ICMP, UDP and OSI

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols			DOD4 Model	
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP		GATEWAY Can be used on all layers	Process	
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT				
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names				
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host	←UDP
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP			Internet	←ICMP
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card —— Switch —— NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers		Network	
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**				

Flooding Attacks

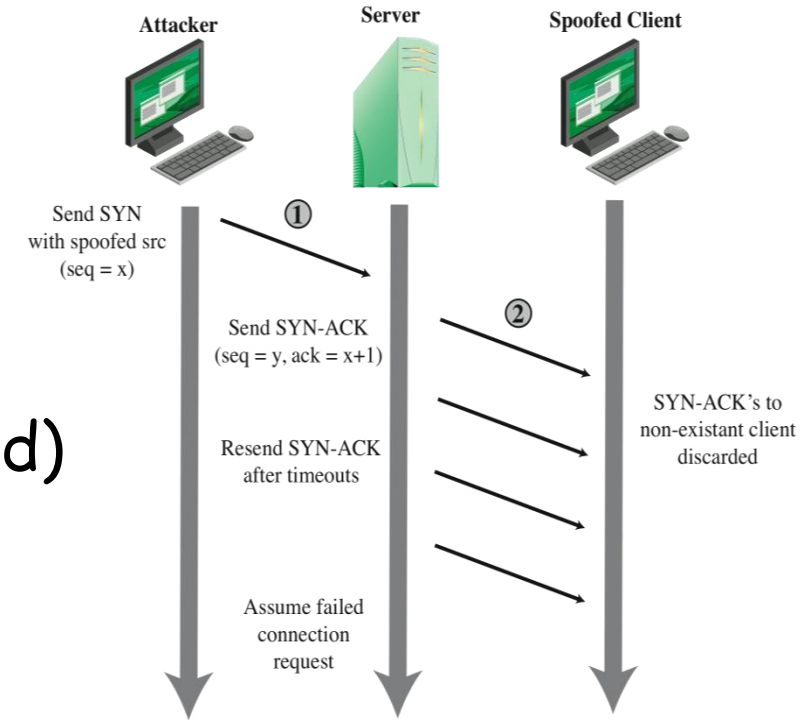
- ICMP flood
  - echo request ("ping") is an ICMP message whose data is expected to be received back in an echo reply ("pong")
  - host must respond to all echo requests with an echo reply containing the exact data received in the request message
  - attacker sends large number of ICMP echo request packets and creates a ping flood
  - traditionally network administrators allow such packets enter into their networks because ping is a useful network diagnostic tool
- UDP flood (User Datagram Protocol)
  - uses UDP packets directed to some port number on the target system
  - as a result, the target system replies with an ICMP Destination Unreachable packet (Type = 3)

Source Address Spoofing

- use forged source addresses - usually via the raw socket interface on operating systems
  - used for custom network testing and still maintained in many current OS
- generates large volumes of packets that have the target system as the destination address
- different random source address
- responses are scattered across Internet; real source is much harder to identify
- backscatter traffic
  - no real system will send legitimate response packets to unused IP address
  - more likely that these IP addresses are spoofed and used for attack
  - **security researchers advertise routes to unused IP addresses to monitor attack traffic**

SYN flooding/Clogging

- attacks the ability of a server to respond to future TCP connection requests by overflowing the tables (allocated state, TCP buffers) used to manage them
  - SYN_RCVD , ESTABLISHED
- thus legitimate users are denied access to the server
- hence an attack on system resources, specifically the network handling code in the operating system
- use spoofed src IP that will not send RST (unused/blocked)



SYN flooding/Clogging - defense

- Block incoming TCP connections from external addresses to internal servers
- Quota per IP
- Remove "half-open"/outdated connections under load periods
- Allocate resources only after ACK
- SYN cookies (client seq#, time, MAC on src, dest IP address, port and time)
  - no need to keep state

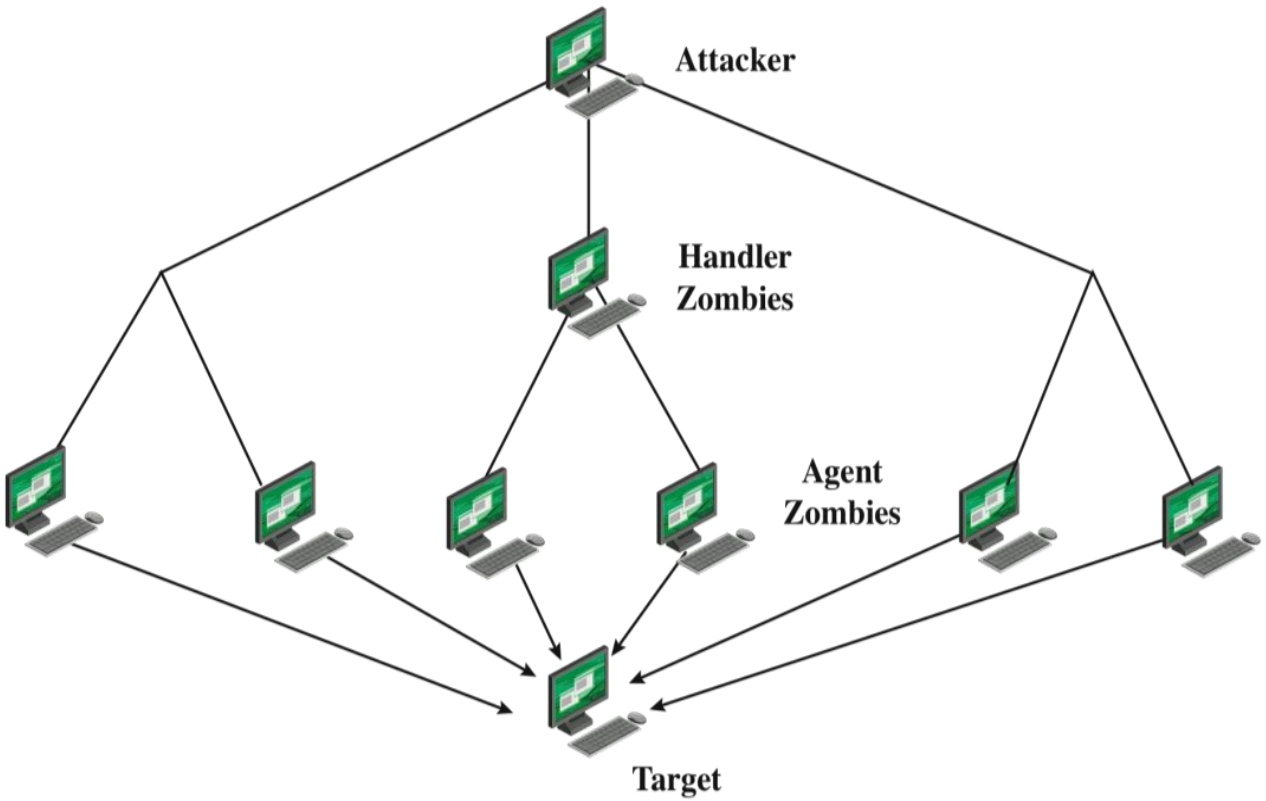
Other attacks

- TCP connection flooding attack
  - establish full TCP connection from valid IPs
- HTTP-based attacks – HTTP flood
  - attack that bombards Web servers with HTTP requests; consumes considerable resources
  - spidering - bots starting from a given HTTP link and following all links on the provided Web site in a recursive way

More DoS attacks

- attacks on mobile devices (battery)
- data availability
- "heavy" legitimate operations
- buffer overflow
  - Remotely crashes a vulnerable system by sending more traffic to a application than it was designed to handle

DDoS Attack Architecture

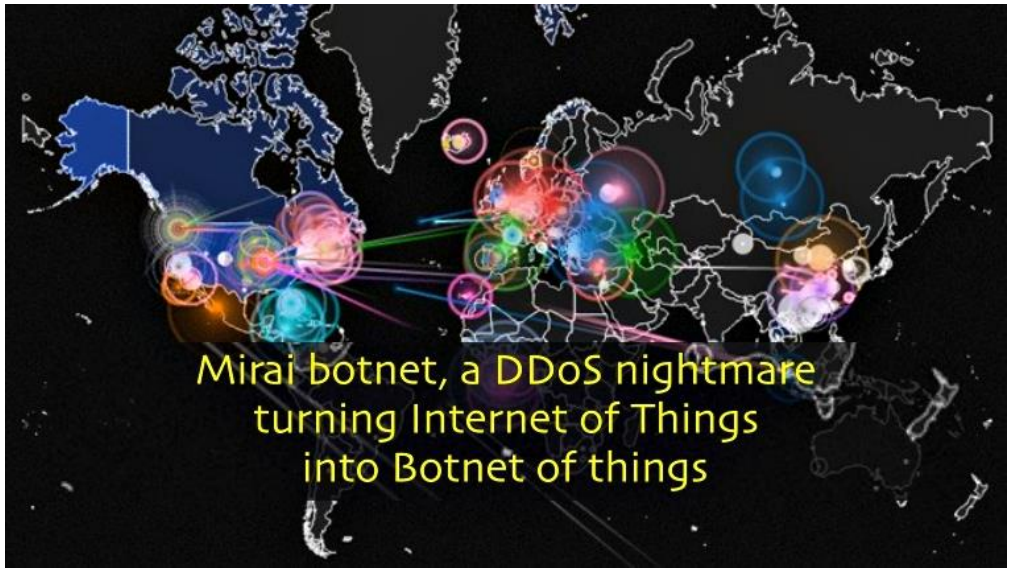


Distributed Denial of Service DDoS Attacks

- Tribe Flood Network (TFN), TFN2K
  - written by aknown hacker named Mixter
  - ICMP flooding, SYN flooding, UDP flooding
  - Unix, Solaris, Windows NT
  - Opened shell in every agent for running handler program
- Trinoo
  - UDP flooding
  - Trinoo is famous for allowing attackers to leave a message in a folder called **cry_baby**
  - The file is self replicating and is modified on a regular basis as long as port 80 is active
- Stacheldraht
  - Combines features of TFN and Trinoo
  - Adds encrypted communication

Dyn DDoS Attack (Oct. 2016)

- multiple DDoS attacks targeting systems operated by Domain Name System (DNS) provider Dyn
- the attack was accomplished through a large number of DNS lookup requests from tens of millions of IP addresses
- executed through the Mirai botnet consisting of a large number of infected IoTs such as printers, IP cameras, gateways and baby monitors

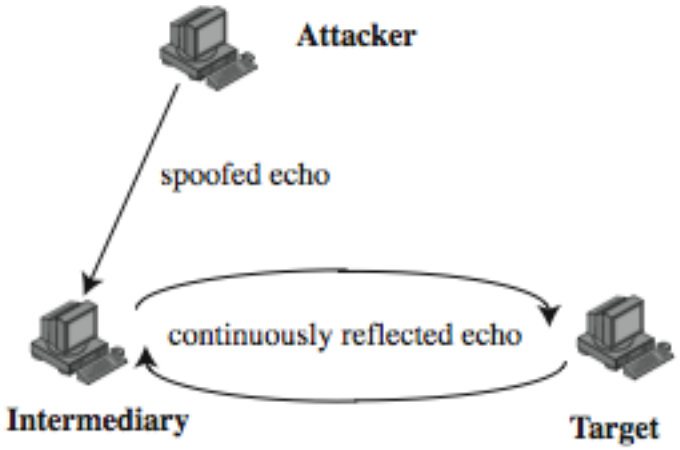


Reflection Attacks

- use normal behavior of network and not "Zombies"
- attacker sends packets to a known service on the intermediary (e.g., server) with a spoofed source address of the actual target system
- when intermediary responds, the response is sent to the target
- "reflects" the attack off the intermediary (reflector)
- goal is to generate enough volumes of packets to flood the link to the target system without alerting the intermediary
- the basic defense against these attacks is blocking spoofed-source packets

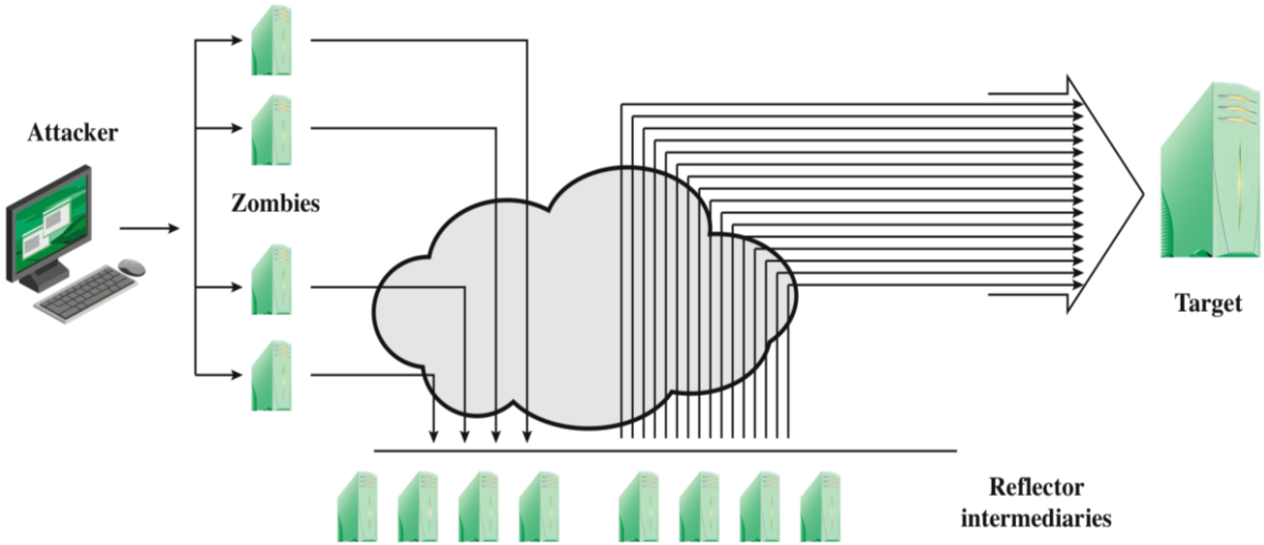
Reflection Attacks

- further variation creates a self-contained loop between intermediary and target
- fairly easy to filter and block



Amplification Attacks

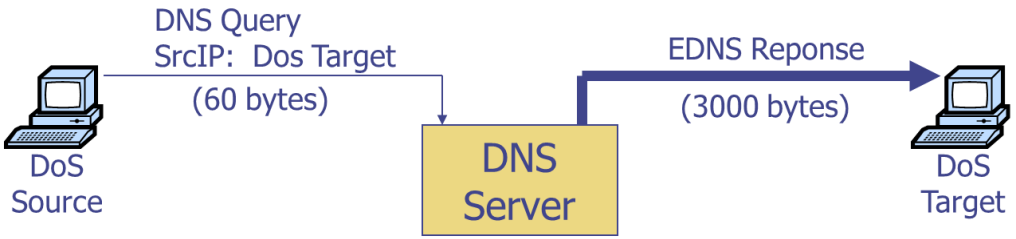
- Smurf (ICMP Packet Magnification) attack
  - the attacker sends an ICMP echo request (ping) to a broadcast address with the victim's source address



DNS Amplification Attacks

- use packets directed at a legitimate DNS server as the intermediary system
- attacker creates a series of DNS requests containing the spoofed source address of the target system
- exploit DNS behavior to convert a small request to a much larger response (amplification)
  - 60 byte request to 512 - 4000 byte response
- target is flooded with responses
- basic defense against this attack is to prevent the use of spoofed source addresses

DNS Amplification attack: (×50 amplification)



DoS Attack Defenses

- these attacks cannot be prevented entirely
- high traffic volumes may be legitimate (popular Web-sites, release of new product…)

- prevention – before attack
- detection and filtering (during)
- traceback (during and after)
- reaction (after)

DoS Attack Prevention

- block spoofed source addresses
  - on routers as close to source as possible
  - filters may be used to ensure path back to the claimed source address is the one being used by the current packet
    - e.g. using Cisco routers command: "ip verify unicast reverse-path"
    - filters must be applied to traffic before it leaves the ISP's network or at the point of entry to their network
- use modified TCP connection handling code
  - cryptographically encode critical information in a cookie that is sent as the server's initial sequence number
    - legitimate client responds with an ACK packet containing the incremented sequence number cookie
  - drop an entry for an incomplete connection from the TCP connections table when it overflows

DoS Attack Prevention

- block IP directed broadcasts (against amplifications)
- limit or block traffic from and into suspicious services and combinations (hostile origin, low reputation ip - alexa)
- manage application attacks with a form of graphical puzzle (captcha) to distinguish legitimate human requests
- ideally have network monitors and IDS to detect and notify abnormal traffic patterns
- use mirrored and replicated servers when high-performance and reliability is required

Responding to DoS Attacks

- identify type of attack
  - capture and analyze packets
  - design filters to block attack traffic upstream
  - or identify and correct system/application bug
- have ISP trace packet flow back to source
  - may be difficult and time consuming
  - necessary if planning to report it the attack to law enforcement agencies.
- implement contingency plan
  - switch to alternate backup servers
  - Set new servers at a new site with new addresses
- update incident response plan
  - analyze the attack and the response for future handling

Computer & Information Security (3-721-460-1)

Security protocols

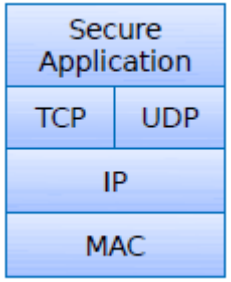
Dept. of Software and Information Systems Engineering, Ben-Gurion University

Prof. Yuval Elovici, Dr. Asaf Shabtai
{elovici, shabtaia}@bgu.ac.il

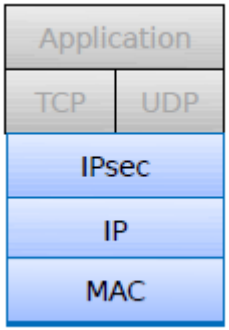
Spring, 2018

Application layer security protocols

- Confidentiality, Integrity, Non-repudiation, Reply, authentication (application layer)
- End-to-end
- Routing and firewall screening is not affected
- Cannot protect against attacks (e.g., Syn attack)
- Updating the application is required
- Examples: PGP, SSH

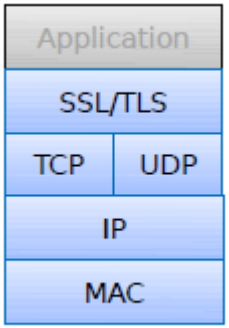


Network layer security protocols



- Confidentiality, Integrity, Reply, authentication (IP level)
- End-to-end / gateway-to-gateway
- Routing is not affected
- Affects firewall screening
- Protects against attack at the transport layer (e.g., Syn attack)
- Transparent to the application
- Examples: IPSec

Transport layer security protocols

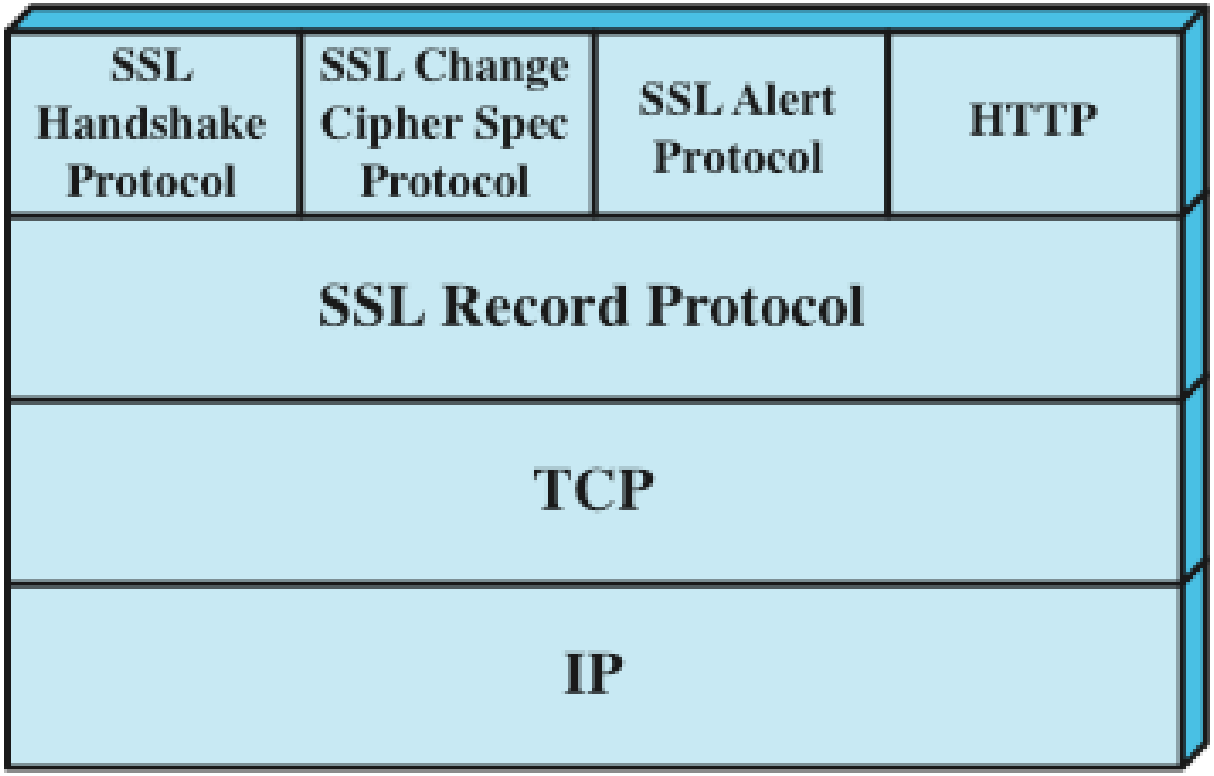


- Confidentiality, Integrity, Reply, authentication
- End-to-end
- Routing and firewall screening is not affected
- Cannot protect against attacks (e.g., Syn attack)
- Transparent to the application
- Examples: SSL/TSL

Secure Sockets Layer (SSL)

- one of the most widely used security services
- transport layer security service - originally developed by Netscape
- general-purpose service implemented as a set of protocols that rely on TCP
- use TCP to provide a reliable end-to-end service
- subsequently became Internet standard RFC2246: Transport Layer Security (TLS)
- may be provided in underlying protocol suite
- or embedded in specific packages

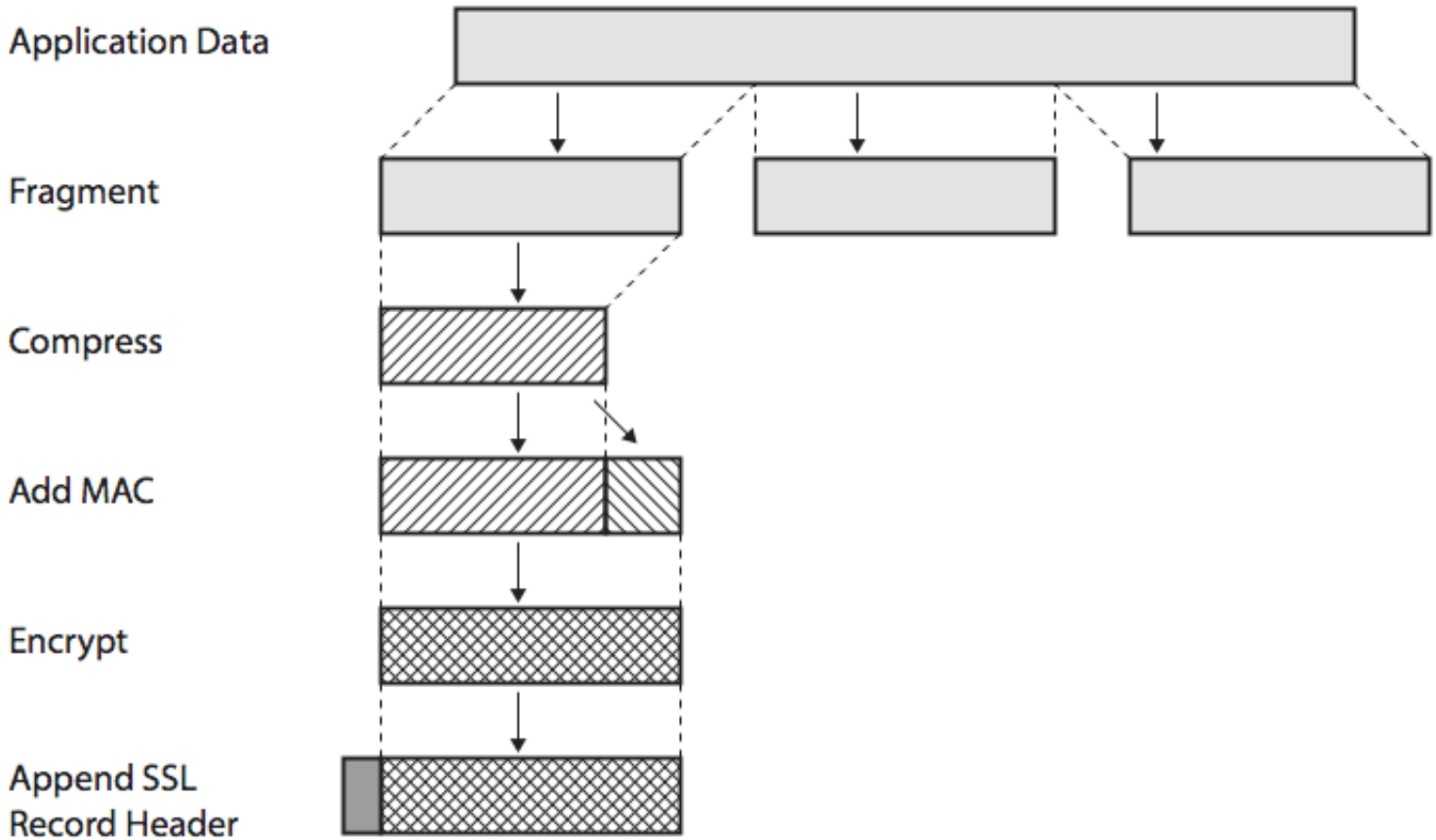
SSL Protocol Stack



SSL Record Protocol Services

- message integrity
  - using a MAC with shared secret key
  - similar to HMAC but with different padding
- confidentiality
  - using symmetric encryption with a shared secret key defined by Handshake Protocol
  - AES, IDEA, RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40, RC4-128
  - message is compressed before encryption

SSL Record Protocol Operation



SSL Change Cipher Spec Protocol

- one of three SSL specific protocols that use the SSL Record Protocol (the simplest)
- consists of a single message which consists of a single byte with the value 1
- sole purpose of this message is to cause pending state to be copied into the current state
- hence updating the cipher suite in use

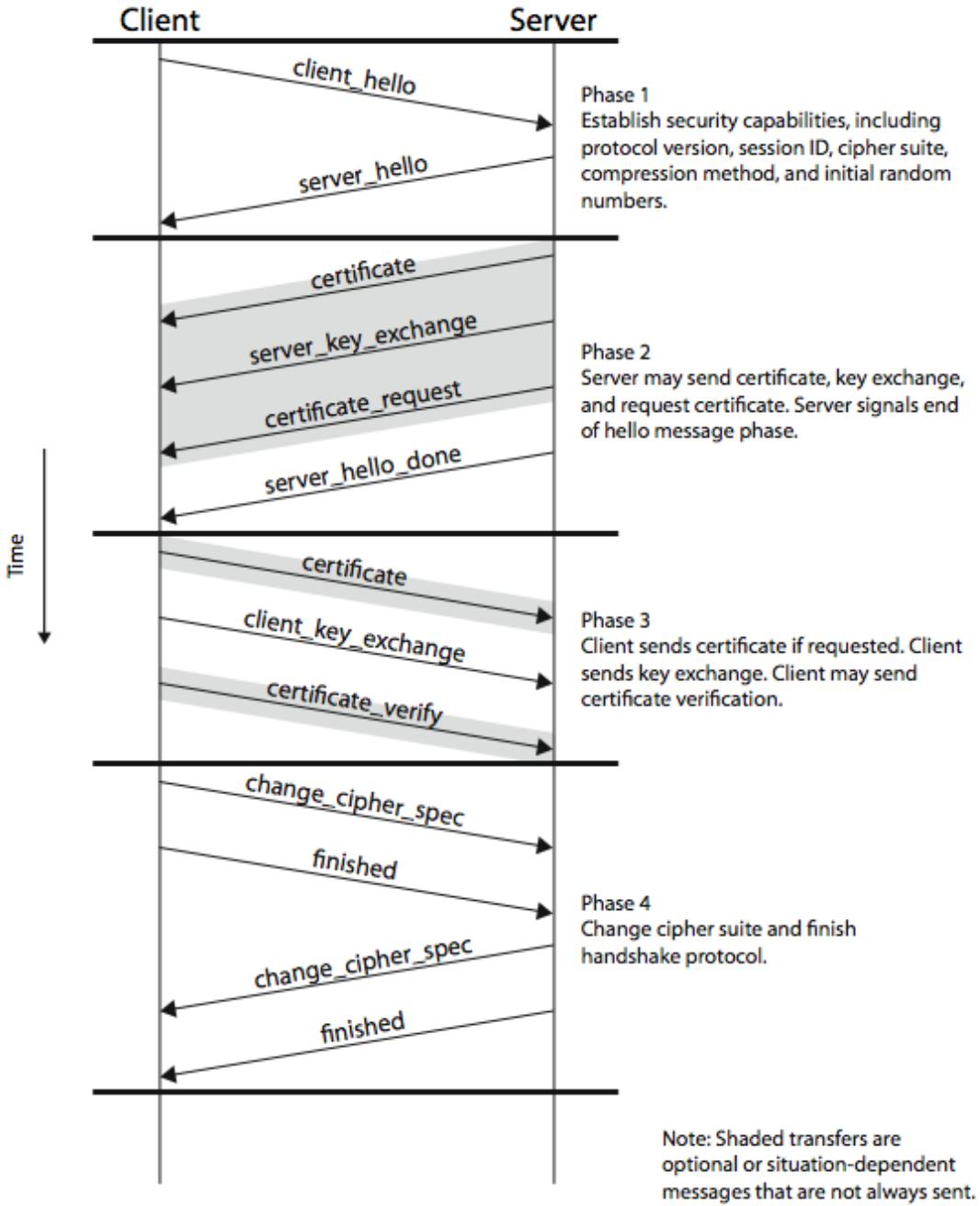
SSL Alert Protocol

- conveys SSL-related alerts to peer entity
- two bytes message: first byte indicating the severity of message - warning (1) or fatal (2); second byte contains a code that indicates the specific alert
- specific alert
  - Fatal (results in immediate termination of the SSL connection): unexpected message, bad record mac, decompression failure, handshake failure, illegal parameter
  - warning: close notify, no certificate, bad certificate, unsupported certificate, certificate revoked, certificate expired, certificate unknown
- compressed & encrypted like all SSL data

SSL Handshake Protocol

- is used before any application data are transmitted
- allows server & client to:
  - authenticate each other
  - to negotiate encryption & MAC algorithms
  - to negotiate cryptographic keys to be used
- comprises a series of messages in phases
  - Establish Security Capabilities
  - Server Authentication and Key Exchange
  - Client Authentication and Key Exchange
  - Finish

SSL Handshake Protocol



Generating the Master Secret

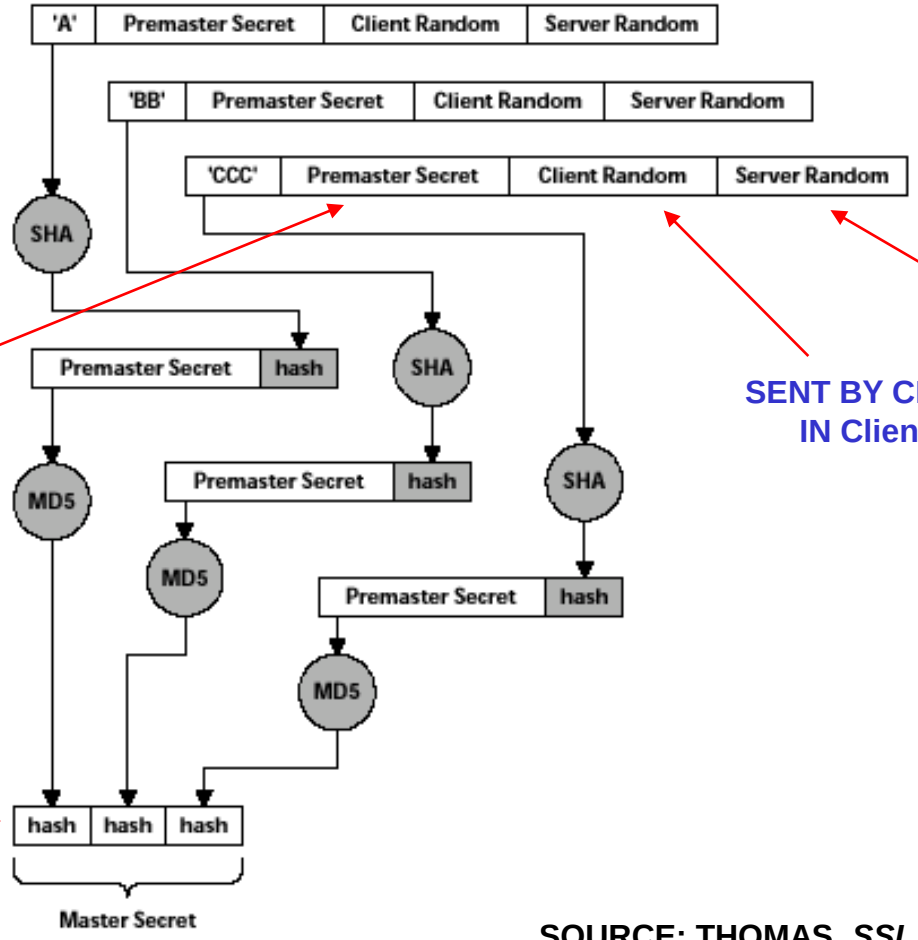
SERVER'S PUBLIC KEY IS SENT BY SERVER IN ServerKeyExchange

CLIENT GENERATES THE PREMASTER SECRET

ENCRYPTS WITH PUBLIC KEY OF SERVER

CLIENT SENDS PREMASTER SECRET IN ClientKeyExchange

MASTER SECRET IS 3 MD5 HASHES CONCATENATED TOGETHER = 384 BITS



SENT BY SERVER IN ServerHello

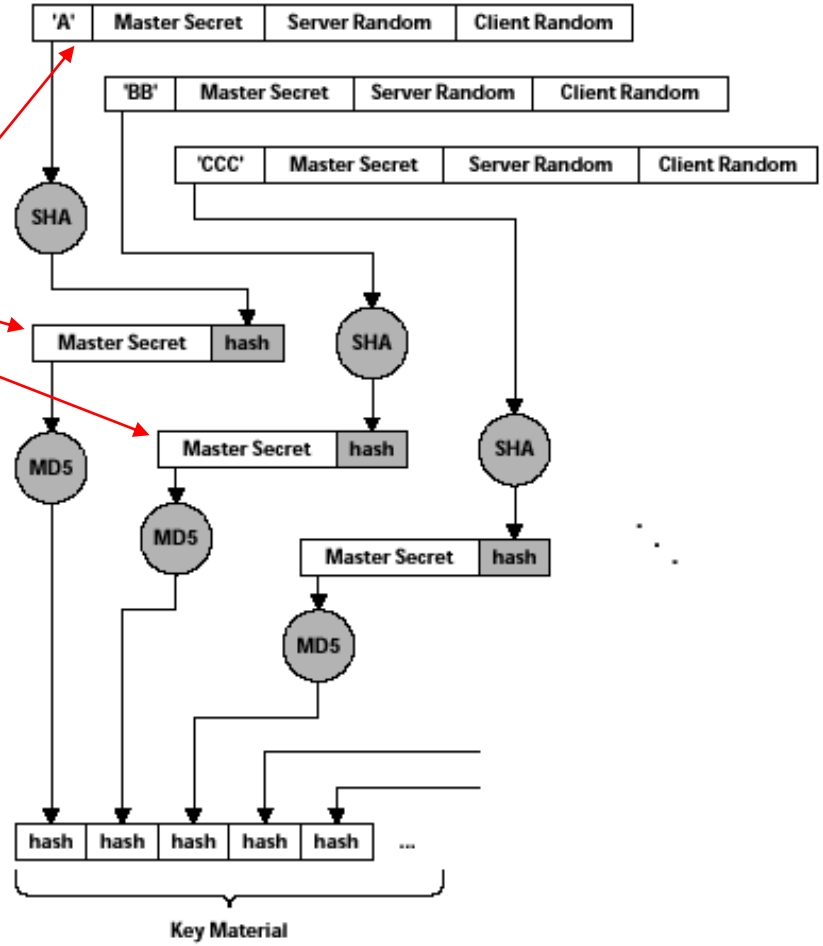
SENT BY CLIENT IN ClientHello

SOURCE: THOMAS, *SSL AND TLS ESSENTIALS*

Generation of Key Material

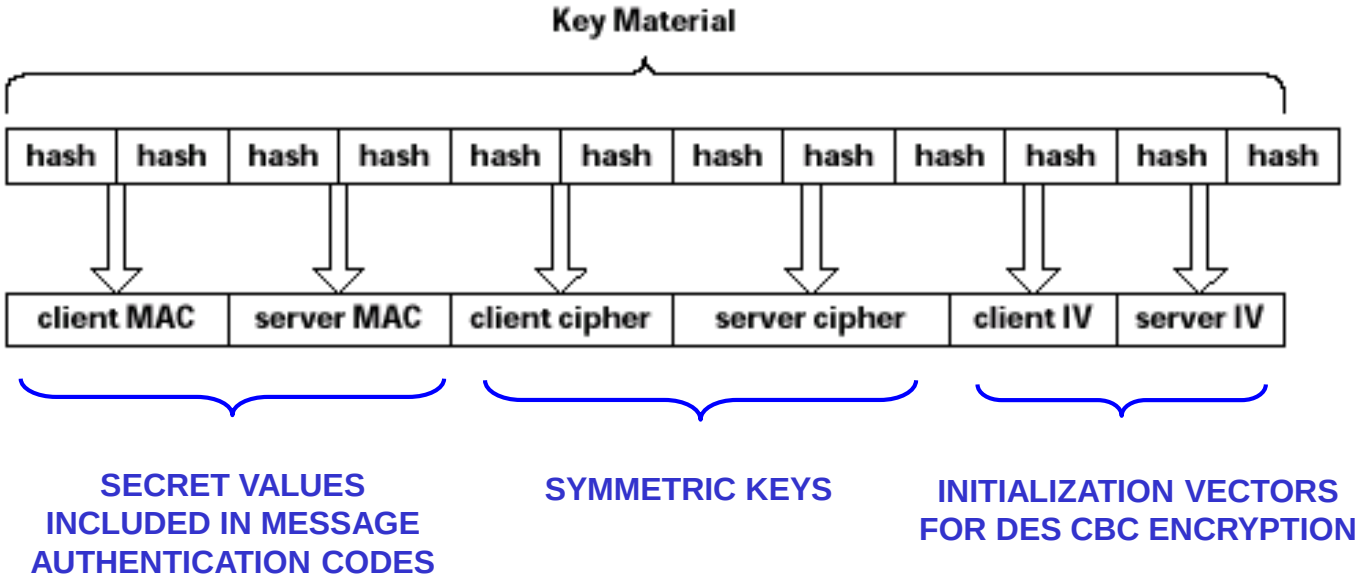
JUST LIKE FORMING THE MASTER SECRET

EXCEPT THE MASTER SECRET IS USED HERE INSTEAD OF THE PREMASTER SECRET



SOURCE: THOMAS, *SSL AND TLS ESSENTIALS*

Obtaining Keys from the Key Material



SOURCE: THOMAS, *SSL AND TLS ESSENTIALS*

HTTPS (HTTP over SSL)

- combination of HTTP and SSL to implement secure communication between a Web browser and a Web server
- built into all modern Web browsers
  - search engines do not support HTTPS
  - URL addresses begin with https://
  - documented in RFC 2818, HTTP Over TLS
  - agent acting as the HTTP client also acts as the TLS client
  - closure of an HTTPS connection requires that TLS close the connection with the peer TLS entity on the remote side, which will involve closing the underlying TCP connection

IP Security (IPsec)

- various application security mechanisms
  - S/MIME, PGP, Kerberos, SSL/HTTPS
- security concerns cross protocol layers
- would like security implemented by the network for all applications
- authentication and encryption security features included in next-generation IPv6
- also usable in existing IPv4

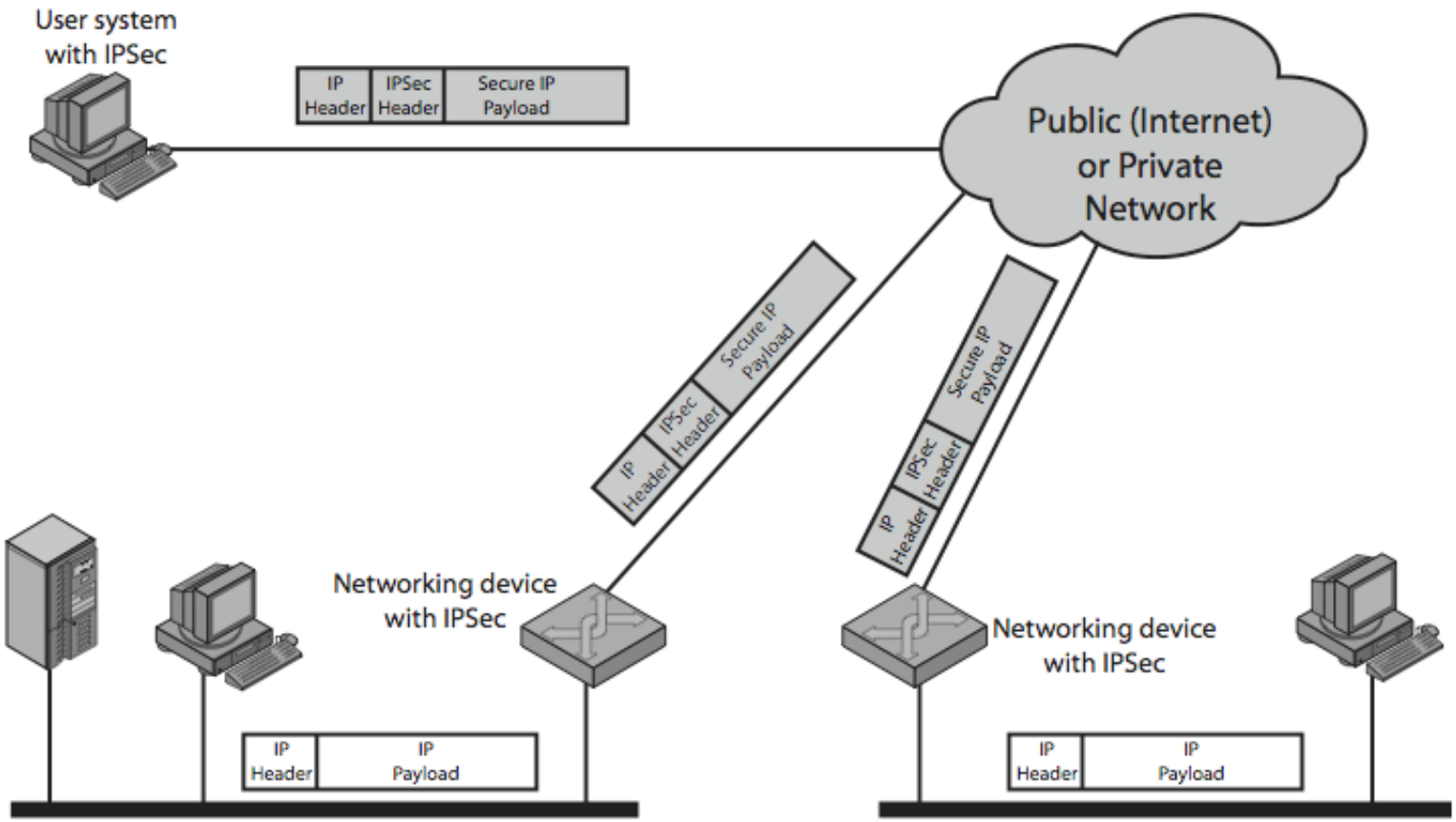
IPsec

- general IP security mechanisms
- provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet

IPsec

- Authentication
  - assures that a received packet was, in fact, transmitted by the party identified as the source in the packet header and that the packet has not been altered in transit
- Confidentiality
  - enables communicating nodes to encrypt messages to prevent eavesdropping by third parties
- Integrity
- Protects against reply attack
- Access control
- Protect against Syn attack and session hijacking

IPSec Uses


User system
with IPSec
IP
Header
IPSec
Header
Secure IP
Payload
Public (Internet)
or Private
Network
Secure IP
Payload
IPSec
Header
IP
Header
Secure IP
Payload
IPSec
Header
IP
Header
Networking device
with IPSec
Networking device
with IPSec
IP
Header
IP
Payload
IP
Header
IP
Payload

Benefits of IPsec

- when implemented in a firewall or router, it provides strong security to all traffic crossing the perimeter
- in a firewall/router it is resistant to bypass
- below transport layer, hence transparent to applications
- can be transparent to end users
- can provide security for individual users
- secures routing architecture

IP Security Architecture

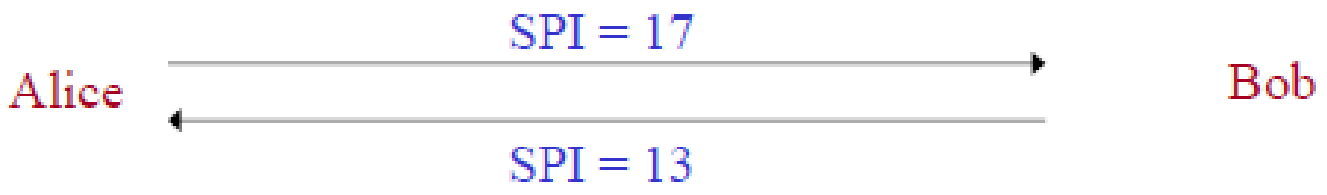
- have three main facilities:
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
  - Key Management / Exchange function
    - concerned with the secure exchange of keys
    - provided by the Internet exchange standard IKEv2
- VPNs want both authentication/encryption
  - hence usually use ESP
- specification is quite complex
  - numerous RFC's 2401/2402/2406/2408

Security Associations

- a one-way relationship between sender & receiver that affords security for traffic flow
- Stored in a database of Security Associations (SAD)
- Can be static (offline) and dynamic by the IKE protocol
- Defined by 3 parameters:
  - Security Parameters Index (SPI)
  - IP Destination Address
  - Security Protocol Identifier
- has a number of other parameters
  - seq no, AH & EH info, lifetime, mode, etc

Security Associations

Protocol = ESP, transport mode,
Encryption Alg.=AES-128, Integrity Alg. = HMAC-SHA256
Life time = 10 Min
SPI = 17
Alice's encryption key =
0xc20c07ab4d2ca5df3027a134d0409416
Alice's integrity key =
0x6cb3df613e590fa095cfa61bebbaf960
Sequence number: 20

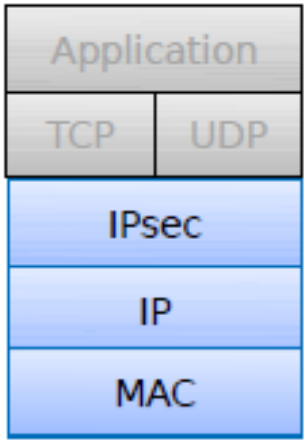


Authentication Header (AH)

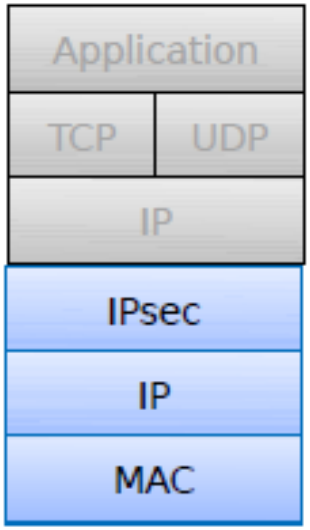
- provides support for data integrity & authentication of IP packets
  - end system/router can authenticate user/app
  - prevents address spoofing attacks by tracking sequence numbers
- based on use of a MAC
  - HMAC-MD5-96 or HMAC-SHA-1-96
- parties must share a secret key

IPSec Header

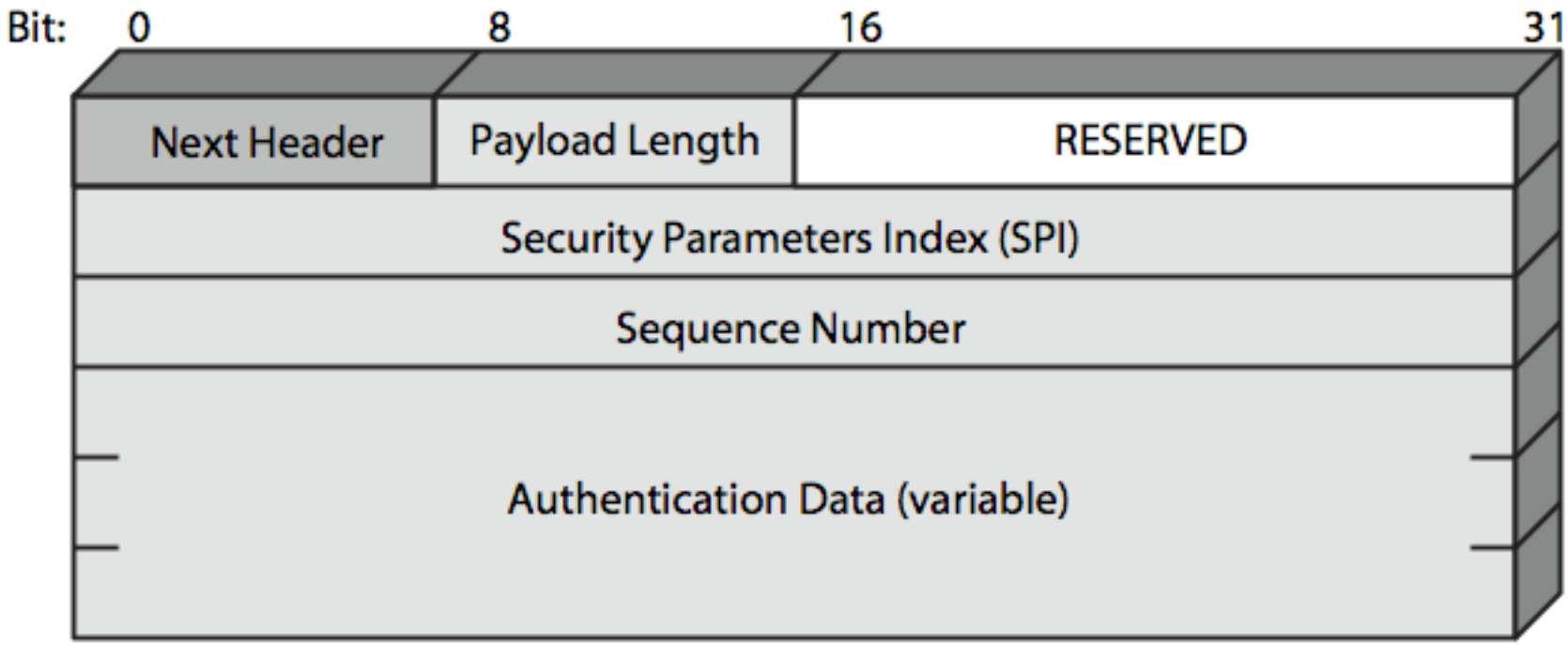
Transport mode



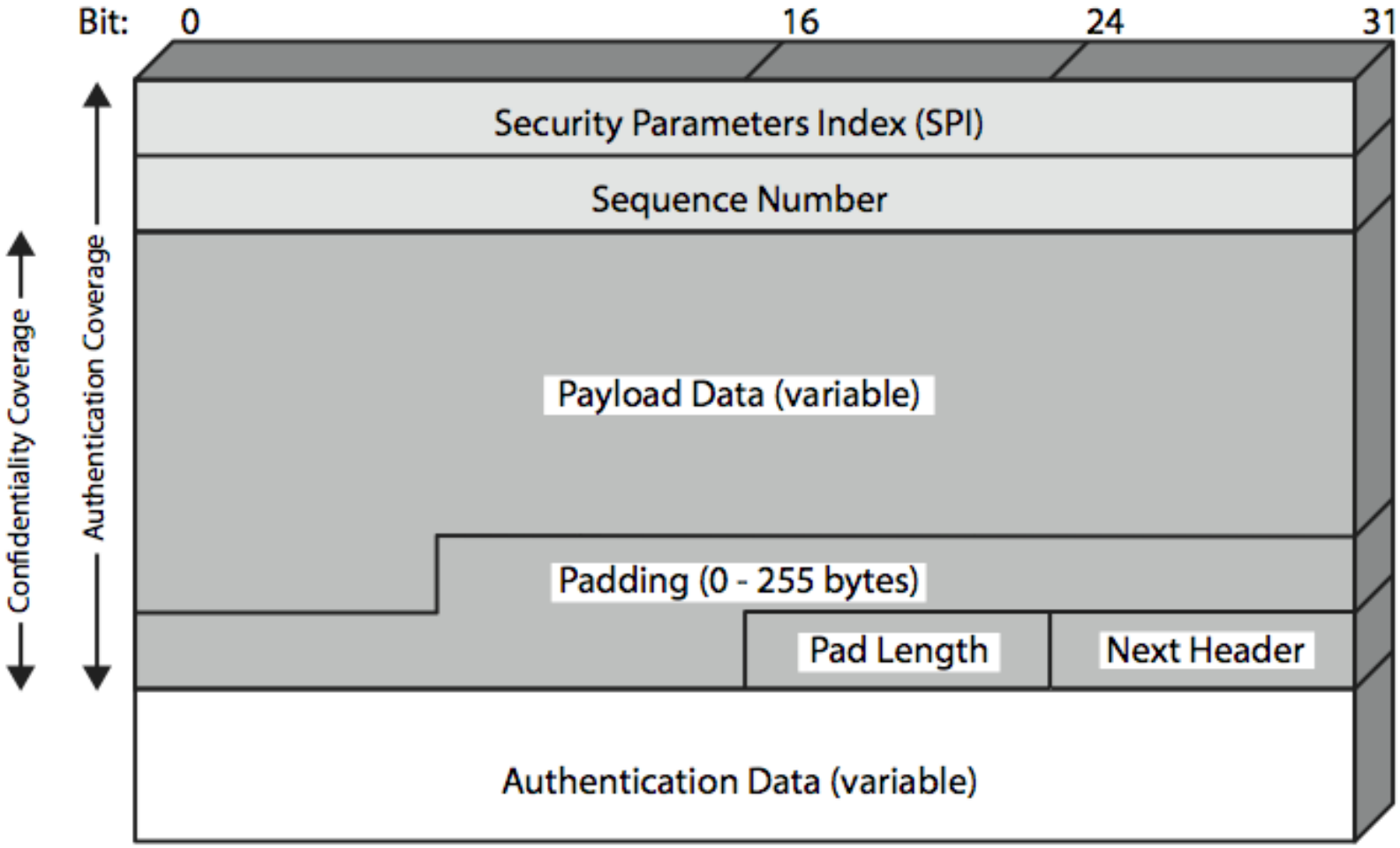
Tunnel mode



Authentication Header



Encapsulating Security Payload (ESP)



Key Management

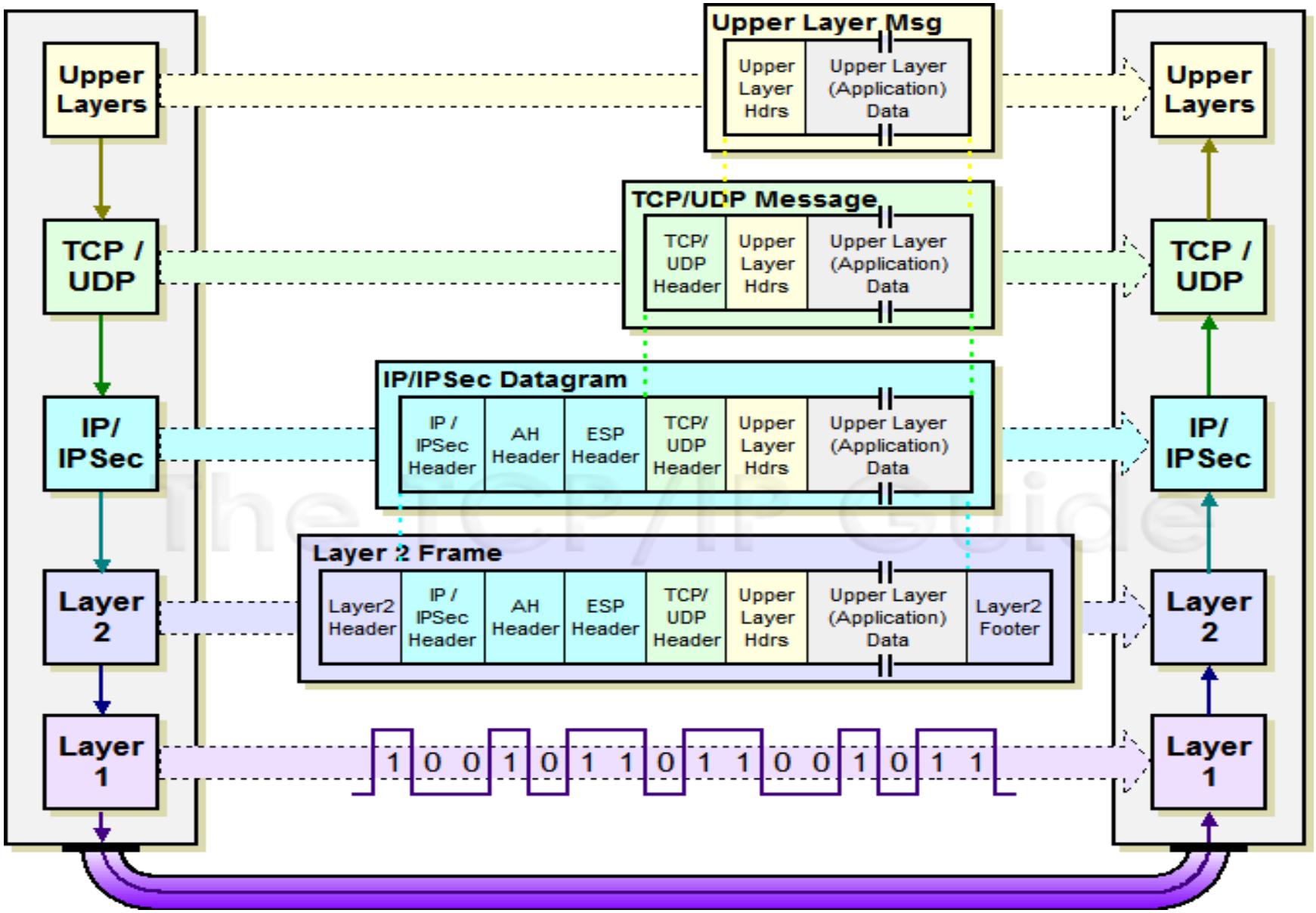
- handles key generation & distribution
- typically need 2 pairs of keys
  - 2 per direction for AH & ESP
- manual key management
  - sysadmin manually configures every system
- automated key management
  - automated system for on demand creation of keys for SA's in large systems
  - has Oakley & ISAKMP elements

Transport and Tunnel Modes

- transport mode protection extends to the payload of an IP packet
- typically used for end-to-end communication between two hosts
- ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header

- tunnel mode provides protection to the entire IP packet
- the entire original packet travels through a tunnel from one point of an IP network to another
- used when one or both ends of a security association are a security gateway such as a firewall or router that implements IPsec
- with tunnel mode a number of hosts on networks behind firewalls may engage in secure communications without implementing IPsec

IPSec Transport Mode: IPSEC instead of IP header



http://www.tcpipguide.com/free/t_IPSecModesTransportandTunnel.htm

IPSec Tunnel Mode: IPSEC header + IP header