SWINBURNE UNIVERSITY OF TECHNOLOGY

Deploying Secure Engineering Applications Online

Protocols

Lecture Five

Outline of Lecture

- This lecture looks at important areas in which digital certificates are used
- Securing web (and other) communications
  - Transport Layer Security (TLS)
- Securing Virtual Private networks
  - IPSec and IKE
- Securing the Domain Name System
  - Domain Name Security Extensions (DNSSEC)

Securing Web Server / Client Communications

- Communications with the web make use of the hypertext transfer protocol (http)
- Usually most sites these days will use a variant of http called https “hyper text transfer protocol secure”
- https makes use of the same messages in http but makes use of a protocol “transport layer security” (TLS) to secure the messages between the client and server
- A series of messages are exchanged between the client and server to establish an authenticated and secure communications channel over which the http messages are exchanged

Transport Layer Security

- Standardised in IETF with RFC 2246 as TLS 1.0
- Now up to TLS 3.0
- TLS provides
  - Privacy
  - Authentication
  - Message integrity
- Operates at the socket layer
  - Above the transport layer
  - TCP three way handshake carried out before TLS handshake

Transport Layer Security

- Application level (In Internet model) protocol
  - secure sockets
  - Requires use of specific ports
  - Specific ports are reserved for each protocol secured by TLS
    - eg HTTPS uses port 443
  - Firewalls need to open these ports
    - end to end
    - An encrypted tunnel
    - cannot proxy or NAT TLS

Transport Layer Security

- Makes use of
  - Digitally signed certificates to authenticate the web server and provide the public key
  - Hashing functions to guarantee integrity of data
  - Encryption to guarantee privacy of data
- Data is encrypted between the browser and the server
- Public key encryption is used for
  - the initial handshake and
  - authenticating the server
  - exchange of symmetric keys (optionally use Diffie-Hellman)
- Symmetric key encryption is used for exchange of data
- Makes possible secure, one-off transactions

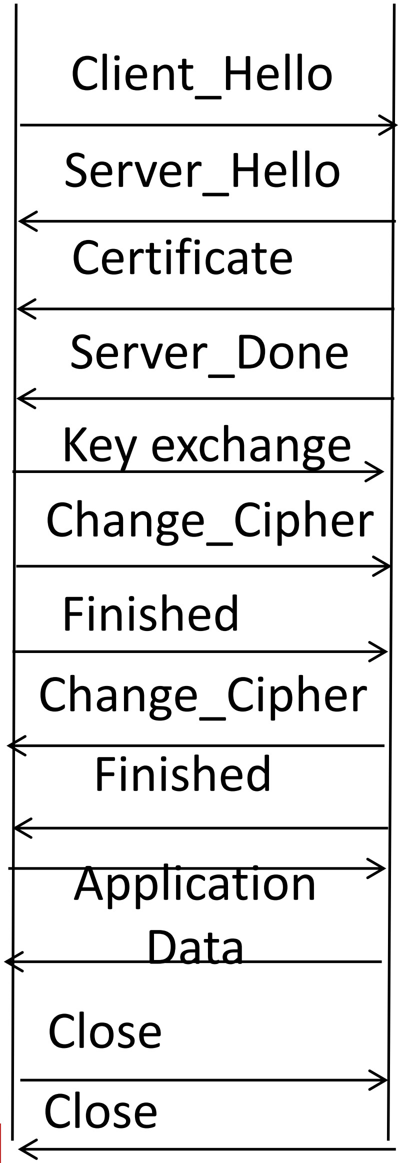
TLS handshake

- Browser and server negotiate cipher suite to use for the rest of the communication
- Browser authenticates the server
  - Server's public key is digitally signed by a trusted 3rd party
  - The browser optionally checks the signature on the server's digital certificate that contains the public key
- Browser generates a random number to be used as the basis of the session key and transmits the random number to the server encrypted with the server's public key
  - Some variants use Diffie-Hellman in this step
- The server decrypts the random number, generates the session key and communicates back to the client that data can now be transmitted

TLS handshake

- Other optional steps include the server authenticating the browser, using digital certificates
- The session key is generated using a hash of the random number and other information exchanged earlier
- Before the SSL / TLS handshake there is the TCP three way handshake to the appropriate port

TLS handshake (most common version)



Negotiate cipher capabilities

Send certificate to client

Random number used for key generation information (encrypted using public key)

After this communications from client encrypted

After this, communications from server encrypted

Transfer of encrypted data

Terminate connection

TLS handshake

- Negotiate cipher capabilities
  - Client sends to server a list of supported symmetric key ciphers and hash functions
  - Server selects which ones to use
- Send certificate to client
  - Server needs to guarantee to client it is who it claims to be
  - Not shown on the diagram is the client verifying the signature contained in the certificate
- Random number exchanged for key generation
  - The example shown uses RSA to share the random number used to form the symmetric key
  - There is another option that uses Diffie-Hellman

TLS handshake

- Change to cipher communications
  - Change_Cipher_Finished messages exchanged
  - From this point onwards all communications is encrypted using symmetric key cryptography
- Finished
  - Setting up the encrypted tunnel is complete
- Application Data exchanged
- Close
  - Both sides send a close message to shutdown the tunnel

TLS ports

Service	Port number	Description
https	443	Hyper-text transfer protocol
ssmtp	465	SMTP mail
snews	563	NNTP news
ssl-ldap	636	ldap directory
spop3	995	POP3 mail
ftps	990	FTP – file transfer

SWINBURNE UNIVERSITY OF TECHNOLOGY

Virtual Private Networks

- Virtual Private Network
  - Makes use of publicly available networking infrastructure to provide the features of a private network
- Definition of VPN according to the IETF
  - An emulation of a private Wide Area Network (WAN) using shared or public IP facilities such as the Internet or private IP backbones
  - An extension of a private intranet across a public network (usually the Internet)
- Originally driven by low cost and wide reach of the Internet
- Recent drivers are avoiding geoblocking and concerns about privacy

Virtual Private Networks

- Key concepts of VPNs are
  - Tunnels
    - Main VPN concept
    - Enables two end-points to exchange data in a way that emulates point to point communication
  - Encryption
    - Enables communication to be confidential even though using shared and very insecure Internet
  - Integrity
    - Ensures data is unchanged
  - Authorisation
    - Specifies what services and resources users can have access to

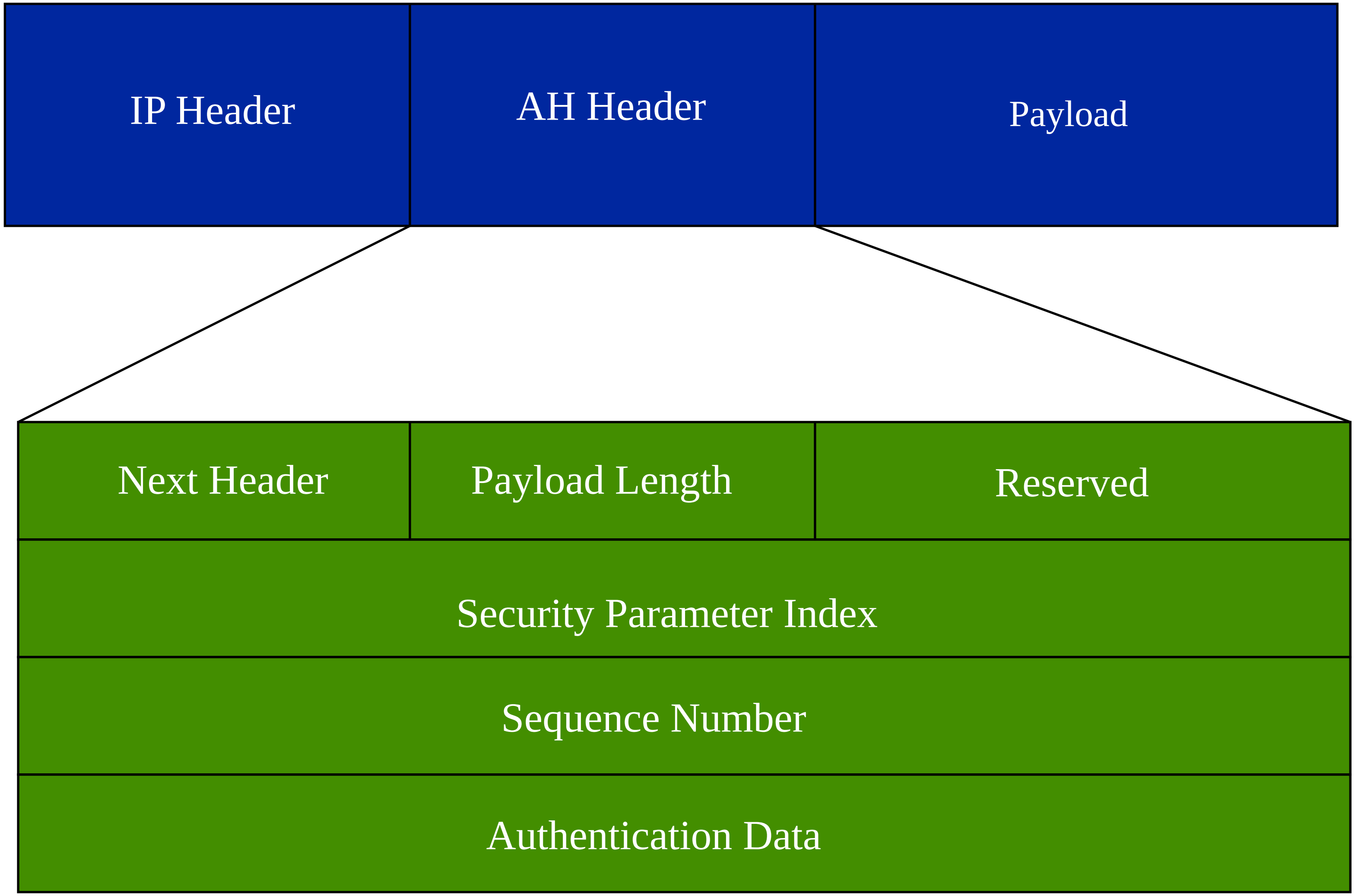
IPSec

- Most widely used VPN technology is IPSect
  - Internet Protocol Security (IPSec)
- A suite of protocols
  - AH: Authentication Header
  - ESP: Encapsulating Security Payload
  - Many others
- Operates at layer 3
  - Tightly integrated with IP
  - Can be used with IPv4
  - Integrated into IPv6
- Very flexible
  - able to integrate into many different authentication and encryption schemes and use many different tunneling technologies

Authentication Header (AH) Protocol

- Used to ensure integrity of packet
  - not confidentiality
- An authentication header is prepended to the payload
- Uses a shared secret key to construct a hash of the contents of the payload
  - Hash based Message Authentication Code (HMAC)
  - Multiple passes of the contents to construct a hashed value (the HMAC)
- Destination uses shared secret key to calculate the hash
  - if the same then payload has not been changed

Authentication Header (AH) Protocol



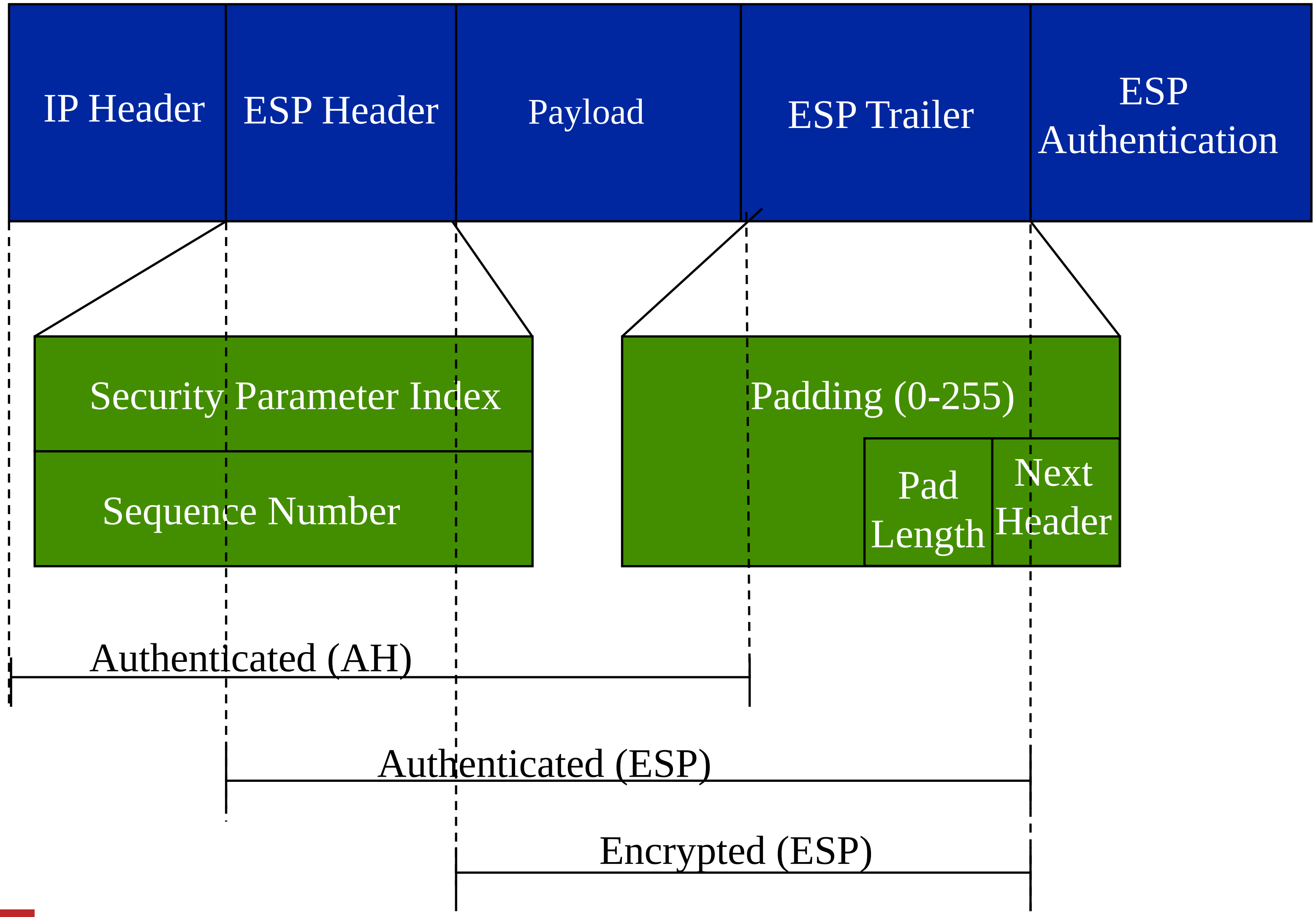
Authentication Header (AH) Protocol

- Next header
  - Protocol number
- Payload length
- Reserved
- SPI
  - index into SAD for Security Association information
- Sequence number
- Authentication data

Encapsulating Security Payload (ESP) Protocol

- Provides both confidentiality AND authentication
- ESP uses encryption for confidentiality and hashing for authentication
- Authentication algorithms used are the same as AH
- Encryption algorithms symmetric
  - use shared secret key
    - CBC-AES, 3DES, IDEA most commonly used
- ESP encrypts and authenticates the payload only

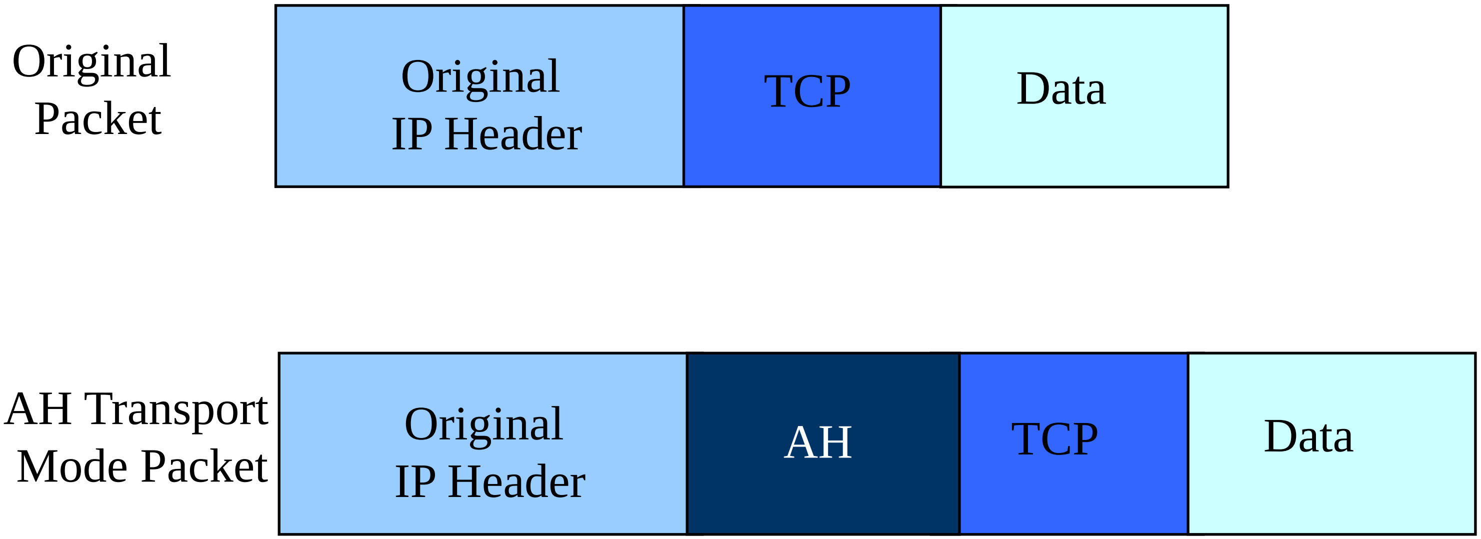
Encapsulating Security Payload (ESP) Protocol



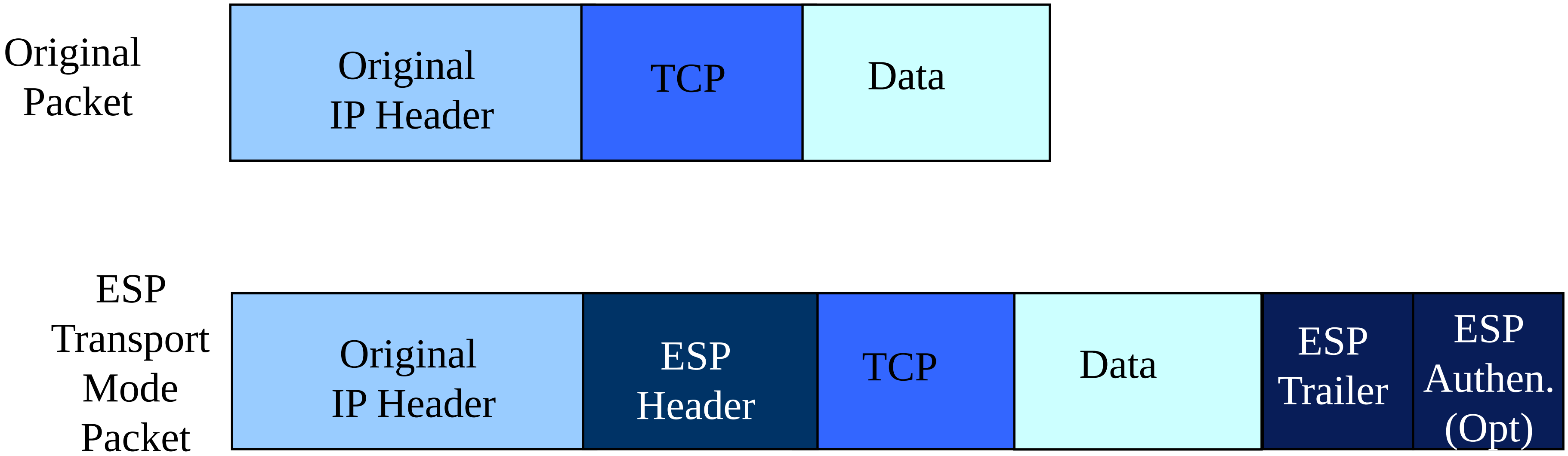
IPSec modes

- IPSec VPNs can operate in two modes
  - Transport mode
    - protects upper layer protocols only
    - IPSec header is inserted between the IP header and the payload
  - Tunnel mode
    - protects the entire IP datagram
    - New IP header is created and the IPSec header is inserted between the new IP header and the old IP header

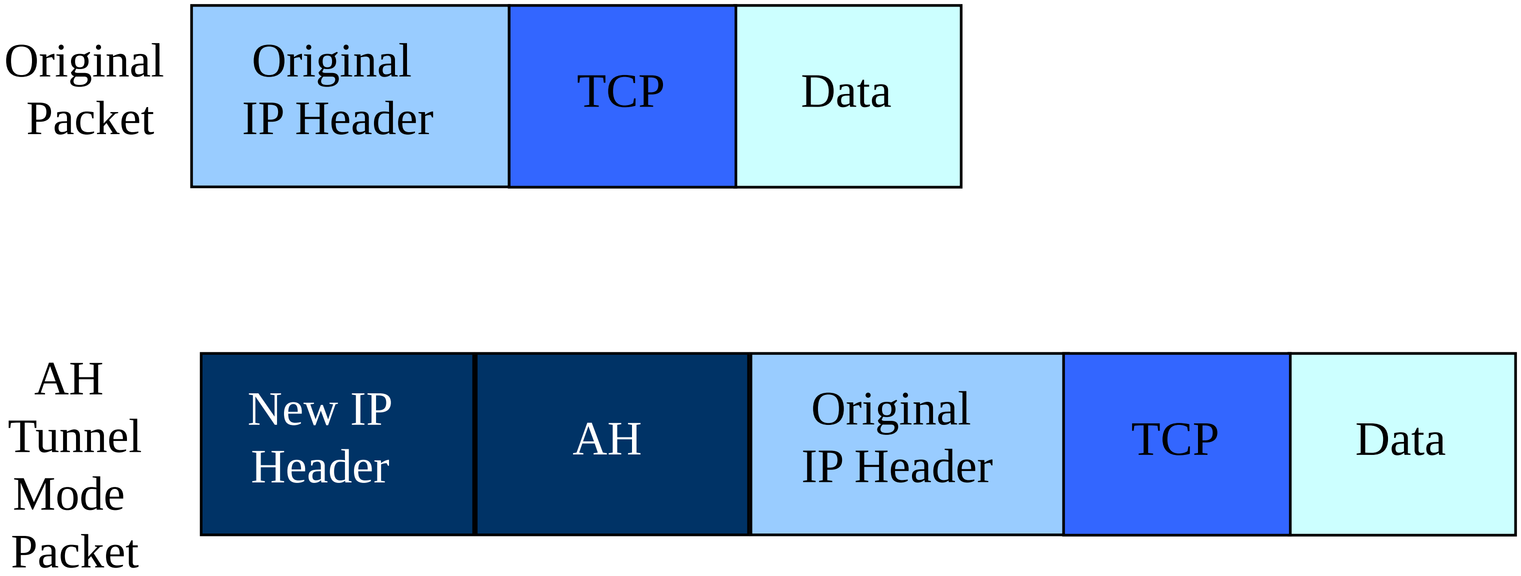
IPSec transport mode with AH



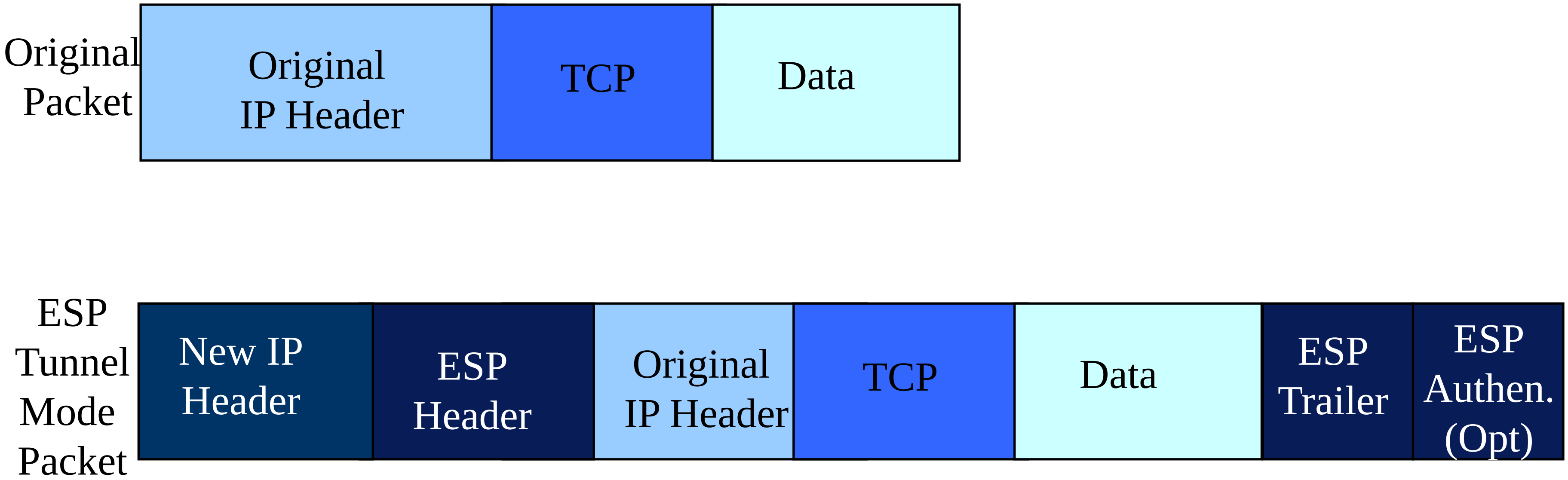
IPSec transport mode with ESP



IPSec tunnel mode with AH



IPSec tunnel mode with ESP



Certificates in IPSec

- Digital Certificates in IPSec are used for
  - Setting up a secure channel for exchange of key information
  - Authentication of VPN client to VPN server
  - Authentication of VPN server to VPN client
- Keys can be distributed manually
  - Changed infrequently
    - not every packet or session
- However, automated key management desirable
  - Large number of users manual key exchange a large overhead
  - Need an automated method of key exchange
  - In IPSec this is done with a protocol called Internet Key Exchange which uses certificates for authentication

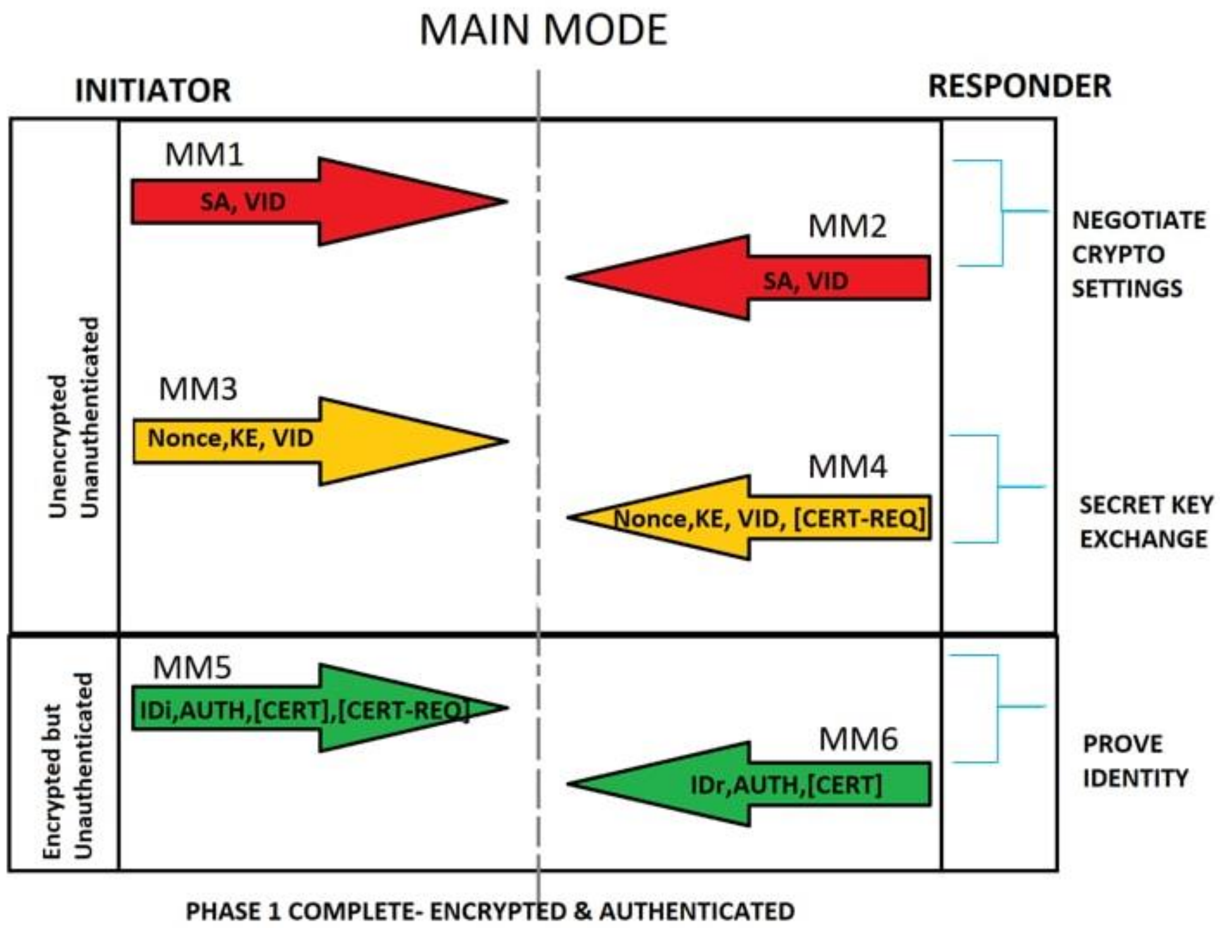
Internet Key Exchange

- IKE has two phases
- IKE phase 1
  - Generates shared secret key using Diffie-Helman hybrid key exchange
  - Enables agreement on which encryption and authentication algorithms to use
  - Ends with authentication of communicating ends through use of Digital Certificates
- IKE phase 2
  - Having established a secure channel for exchanging keys, the actual IPSec VPN is then set up in phase 2

IKE (Main Mode)

- Phase 1 has a number of different modes where information is embedded in other messages
  - Most important (and simplest to understand) is the Main Mode
- Consists of a number of exchanges of messages
  - First two messages are used for negotiating the security policy for the exchange
  - The next two messages are used for the Diffie-Hellman keying material exchange.
  - The last two messages are used for authenticating the peers with signatures or hashes and optional certificates
    - These last two authentication messages are encrypted with the previously negotiated key and the identities of the parties are protected from eavesdroppers.

Main Mode Message Exchange



From https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/217432-understand-ipsec-ikev1-protocol.html

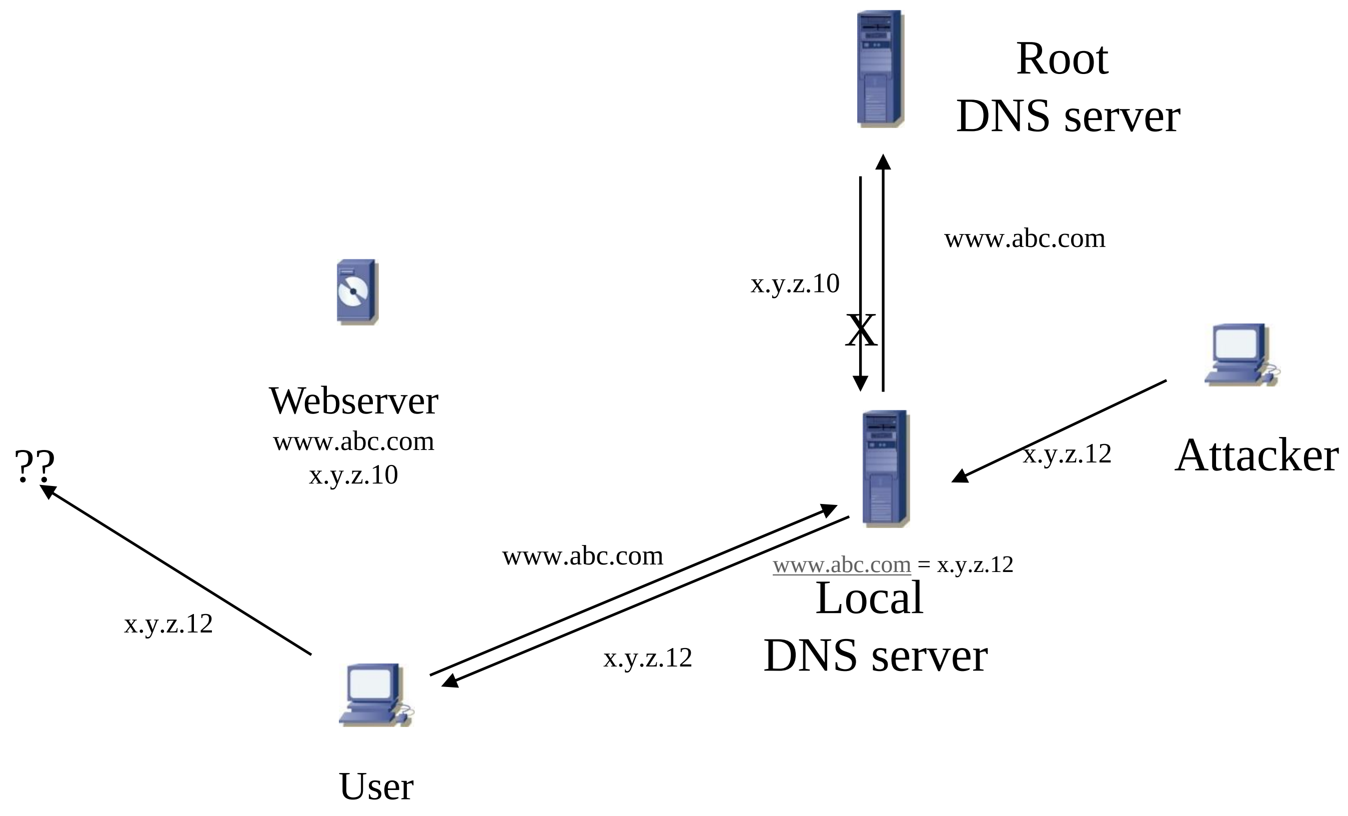
Domain Name System (DNS)

- The DNS is essential for the running of the Internet
- It provides a way of mapping between IP addresses and domain names
  - Eg swin.edu.au is a domain name with corresponding IP address of 136.186.1.10
- The DNS is a hierarchical system of DNS servers (Resolvers) where if a resolver does not know a domain name, it refers it to a higher level resolver
- This in turn may refer it to other high level resolvers until the name is found

DNS Attacks

- The DNS is vulnerable to a cache poisoning attack
  - DNS server asks a root server to resolve an unknown domain name
  - Attacker transmits bogus response to request
  - DNS server caches bogus response
  - Domain name resolutions to that server return an invalid IP address resulting in a denial of service

DNS Denial of service



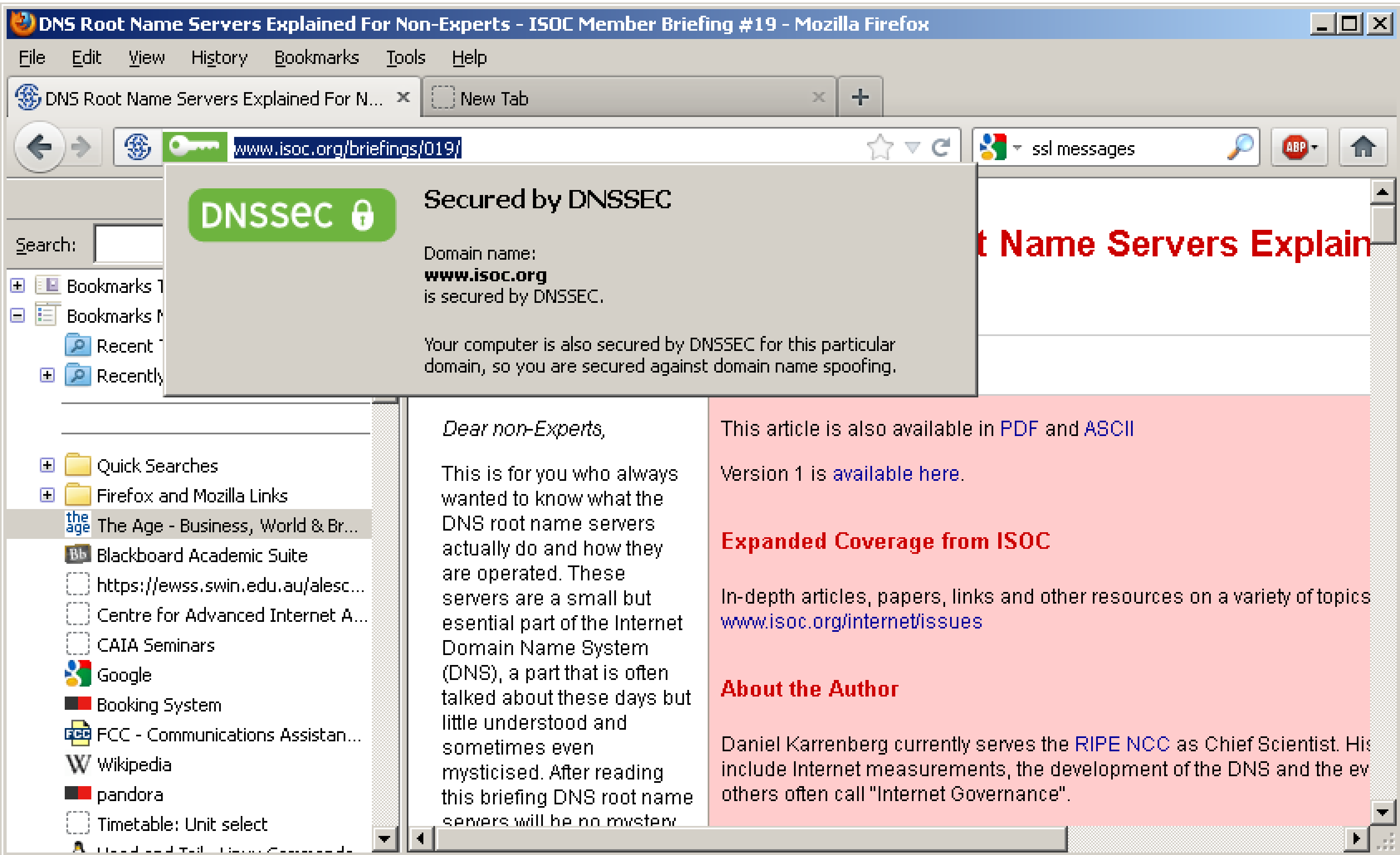
DNS Security Extensions

- The importance of DNS has increased over the past ten years
- Identity of hosts on the Internet used to be defined by their IP addresses
  - NAT extended to the carrier level has made that much less the case
  - IP addresses are now temporary tokens that are linked to an object for the duration of the transaction
  - Good discussion on the topic here
    - http://www.potaroo.net/ispcol/2015-08/gvi.html
- Much of the functionality that used to be provided by IP addressing is now being filled by fully qualified domain names
- Where identity needs to be maintained, DNS (rather than IP address) increasingly fills that role
  - Consequent increase in the importance of DNS integrity

DNS Security Extensions

- DNSSEC goal is to provide origin authentication to DNS clients (resolvers) so as to prevent forged DNS data being sent to the resolver
- All responses from the DNS Server are digitally signed
- Does not provide confidentiality, solely aimed at providing integrity
- Top level of DNS (the DNS root zone) is the Certificate Authority
  - More information as well as browser plug-ins at http://www.internetsociety.org/deploy360/dnssec/basics/

DNS Security Extension



Conclusion

- This lecture looked at some of the important technologies that make use of certificates for authentication
- We looked at
  - TLS primarily (but not exclusively) used for securing web communications
  - IKE and IPSec used for establishing Virtual Private Networks in the Internet
  - DNSSec used to secure the Domain Name System