UNIVERSITY OF DERBY

5CC515 – Networks and Security
Lecture 7: Security Essentials

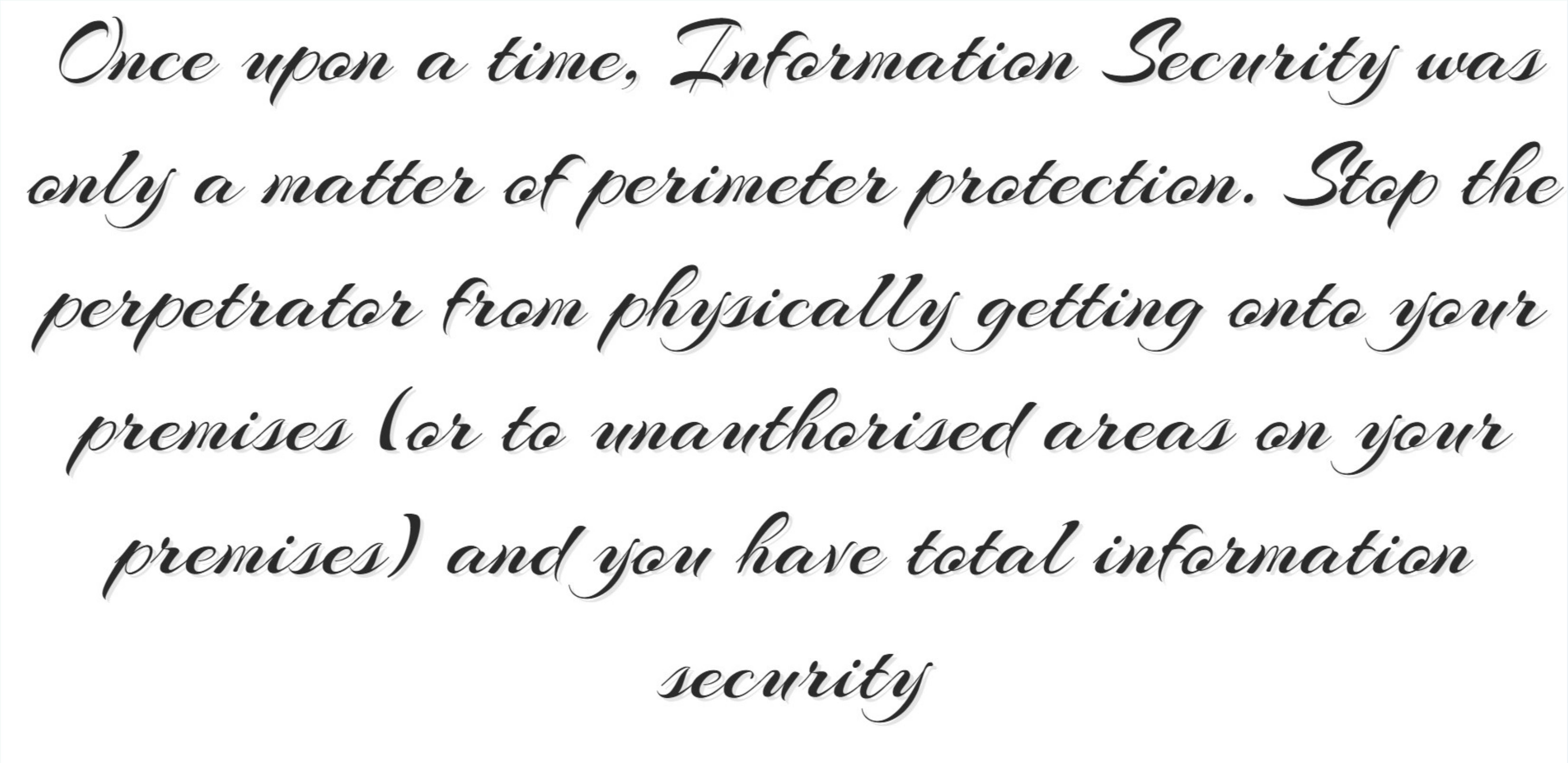
derby.ac.uk

Sensitivity: Internal

Background

- Information security requirements change with the advance in technology
- Traditional security is provided by physical and administrative mechanisms
- Computer security requires new applications of these such as automated tools to protect stored information
- Networks and data storage systems require additional protection on the communications link and at the end point.

A long time ago…



Once upon a time, Information Security was only a matter of perimeter protection. Stop the perpetrator from physically getting onto your premises (or to unauthorised areas on your premises) and you have total information security

… and now…

- Security in the current context means:
  - Information systems security
  - Cryptography
  - Encryption
  - Confidentiality
    - Authentication
  - Integrity
    - Auditing
    - Authorisation
  - Availability
  - Nonrepudiation

- Our perpetrators are:
  - External and internal attackers
  - Our own systems
- For those of you who like videos:
  - 10 Essential Security Practices
  - What would Google do

… but it is rare, right?

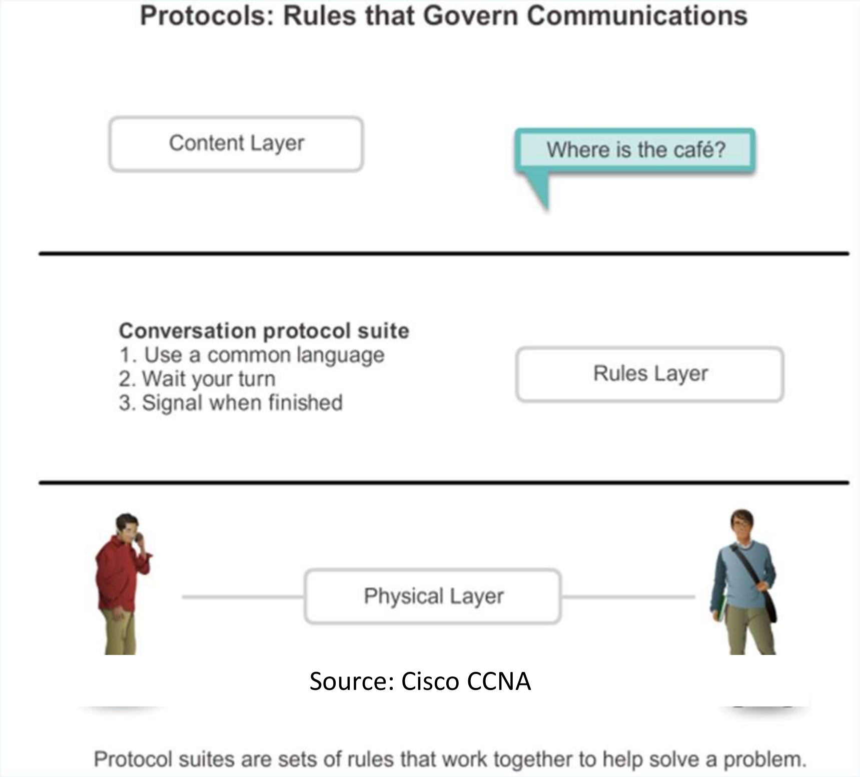
- No, security breaches are common and now well reported on
- Some you might remember:
  - Equifax (2017)
  - CEX (2017)
  - Deloitte (2017)
  - Pizza Hut (2017)
  - Bupa (2017)
  - Wonga (2017)
  - In fact here is a list of 27 famous ones:
  - Government paper on security breaches
- … 2020
  - July – Twitter
  - April – Zoom
  - April – Magellan Health
  - March – Marriott
  - February - MGM

Well at least its only online…

- HMRC
  - 21st November 2007, HMRC 2CDs containing:
    - 25 million records of
      - Names
      - Addresses
      - dates of birth
      - child benefit numbers
      - National Insurance numbers
      - bank or building society account details.
  - Password protected but not encrypted
  - Effects were that:
    - 1000s of citizens closed and reopened bank accounts
  - Security became a matter of huge concern, story was followed by numerous similar stories in the press
  - Head of HMRC resigned

- … but they learned right?
- 4204 data losses in 2019-20
- Mostly from improperly secured devices outside of offices
- 25 classed as severe

Protocols: rules that govern communications



Protocols: Rules that Govern Communications

Content Layer

Where is the café?

Conversation protocol suite

1. Use a common language
2. Wait your turn
3. Signal when finished

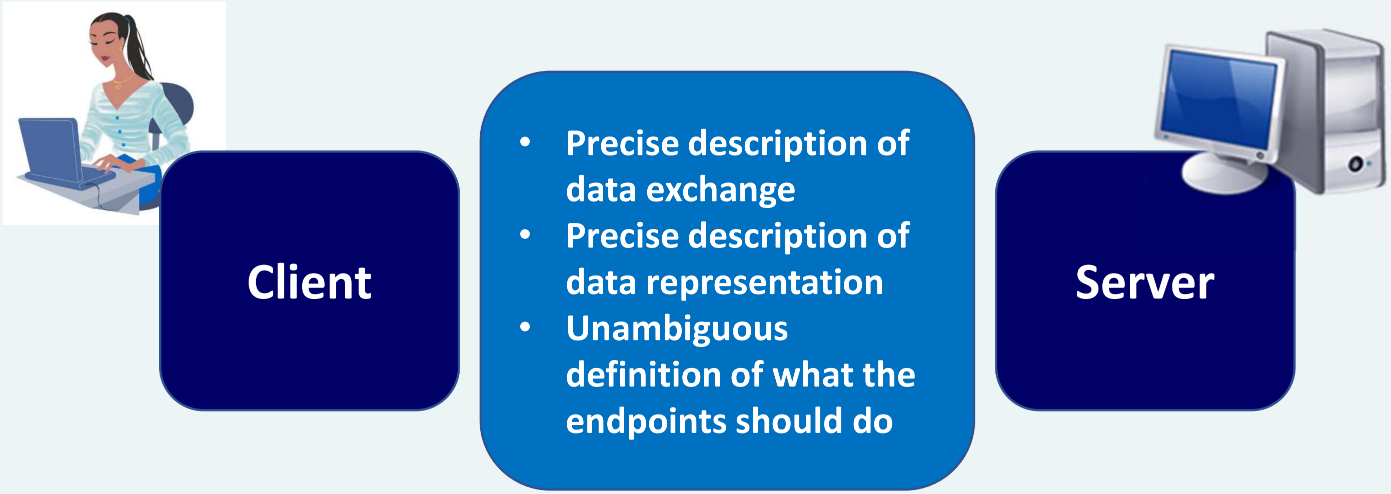
Rules Layer

Physical Layer

Source: Cisco CCNA

Protocol suites are sets of rules that work together to help solve a problem.

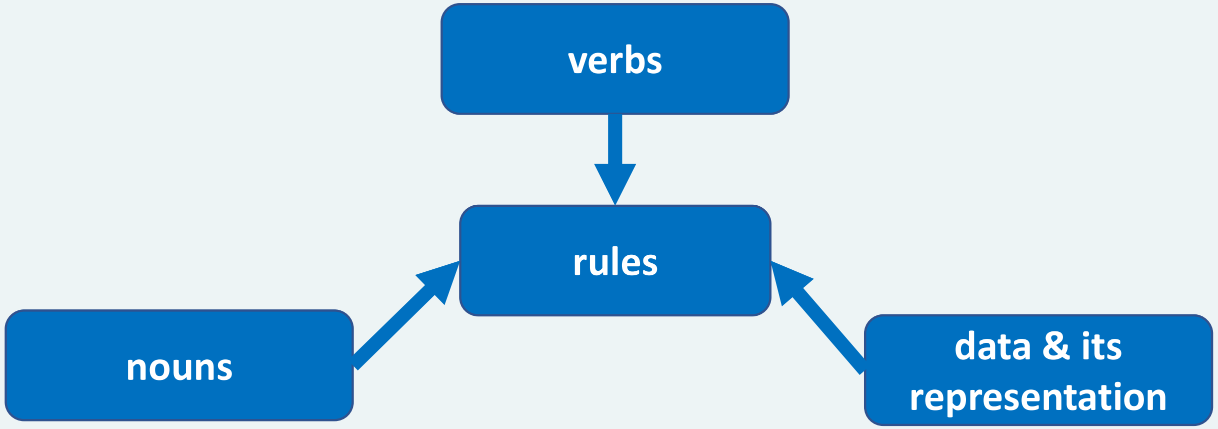
Rules' layer in client-server protocols



- Precise description of data exchange
- Precise description of data representation
- Unambiguous definition of what the endpoints should do

Basic components of a client-server protocol

- They also define rules which bring together
  - ‘commands’ → verbs and nouns
  - data protocol units → e.g., bits, frames, packets, segments, data
  - data representation → e.g., 00-B0-D0-86-BB-F7, 192.168.1.1, 80



Sensitivity: Internal

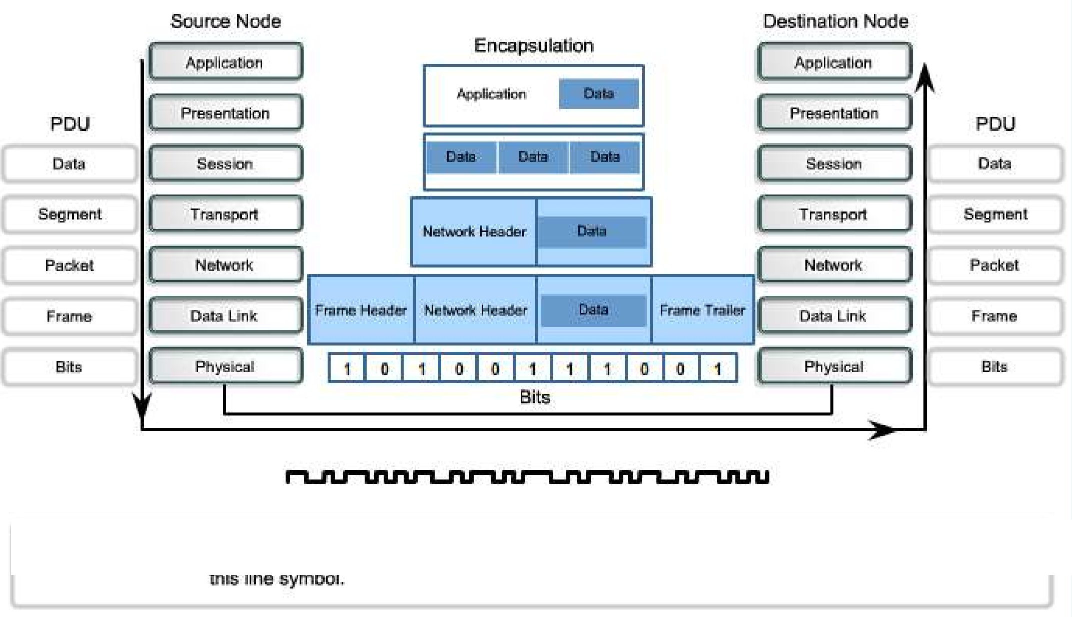
Network security protocols and the OSI model

HTTPS, S/MIME, RADIUS

SSL/TLS

IPSec, VPN

PPP



Session id

Port, seq. nr.

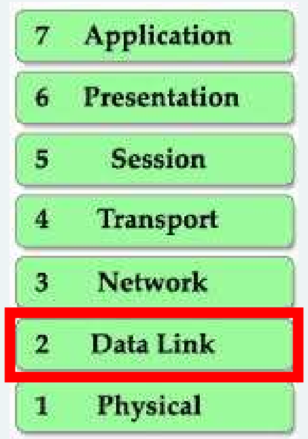
IP address

MAC address

Source: Cisco CCNA

PPP protocol

- Provides security for direct node-to-node communication through a serial link
- Allows two modes for authentication: PAP or CHAP
  - both modes rely on lookup of pre-shared secret passwords



7 Application

6 Presentation

5 Session

4 Transport

3 Network

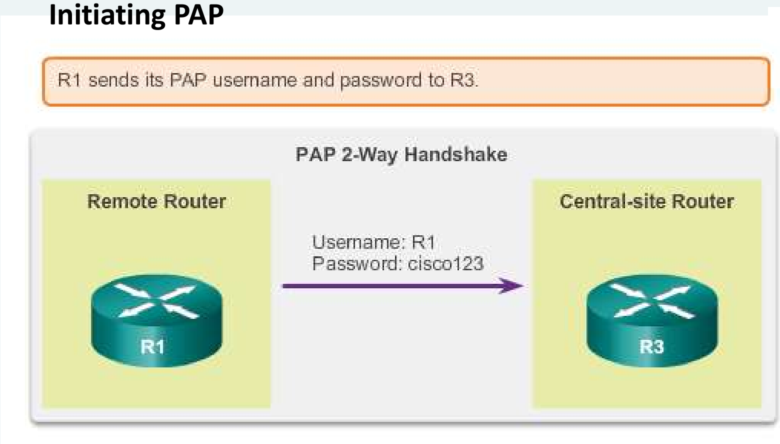
2 Data Link

1 Physical

PAP: Password Authentication Protocol

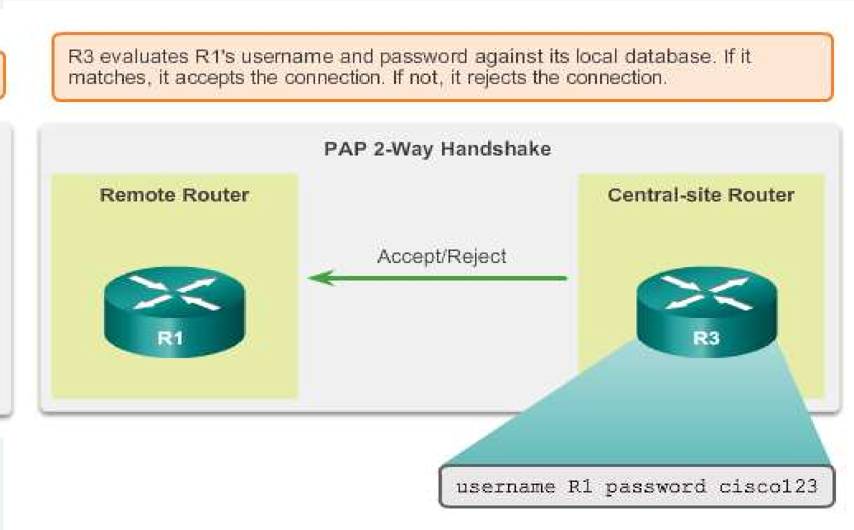
- Password and username are sent repeatedly in plain text
- Receiver authenticates and acknowledges authentication using ack message

Initiating PAP



R1 sends its PAP username and password to R3.

Completing PAP



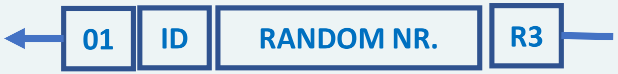
R3 evaluates R1's username and password against its local database. If it matches, it accepts the connection. If not, it rejects the connection.

```
username R1 password cisco123
```

https://en.wikipedia.org/wiki/Password_Authentication_Protocol

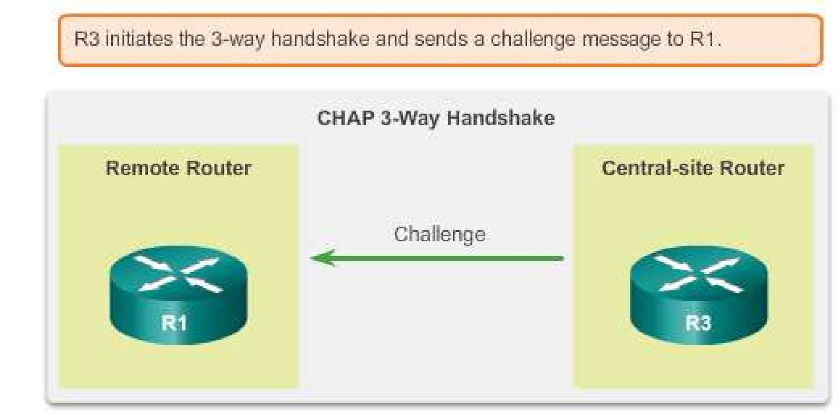
CHAP: Challenge Handshake Authentication Protocol

COMPONENTS OF CHALLENGE PACKET



- Both systems know a shared secret
- Device challenges connecting device – One way hash of challenge + secret is sent back
- Challenge is repeated at random intervals
- Resilient to replay attacks (due to random number and packet id)

Initiating CHAP

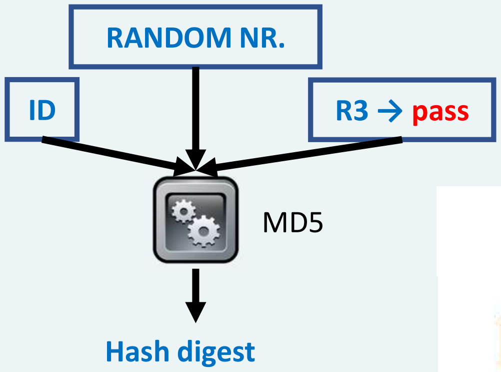

R3 initiates the 3-way handshake and sends a challenge message to R1.

Source: Cisco CCNA; RFC 1994

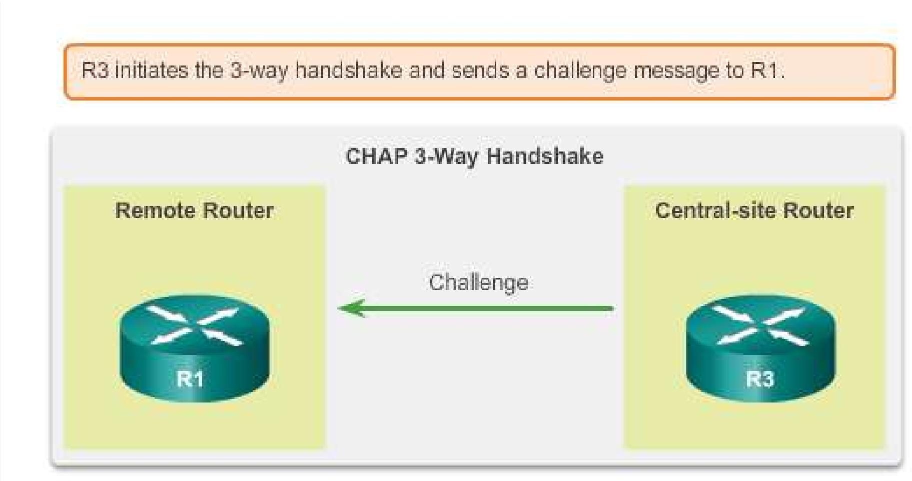
R3 initiates the 3-way handshake and sends a challenge message to R1.

https://en.wikipedia.org/wiki/Challenge-Handshake_Authentication_Protocol

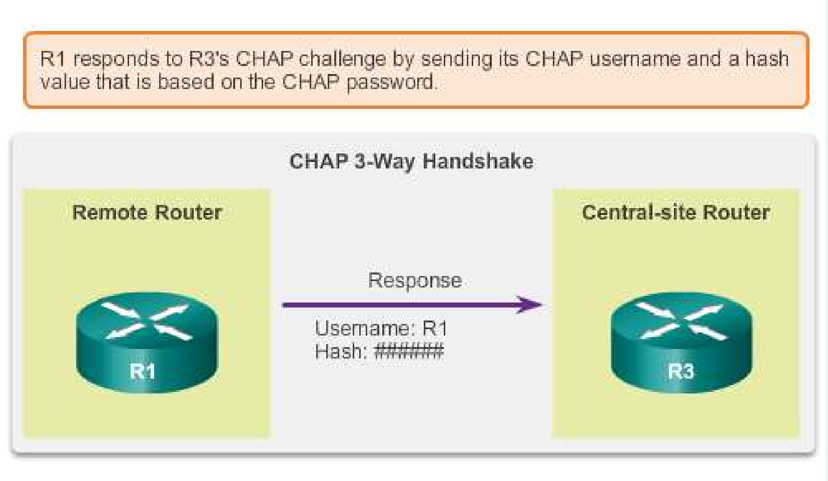
CHAP: Challenge Handshake Authentication Protocol (1)



PROCESSING OF CHALLENGE PACKET


R3 initiates the 3-way handshake and sends a challenge message to R1.

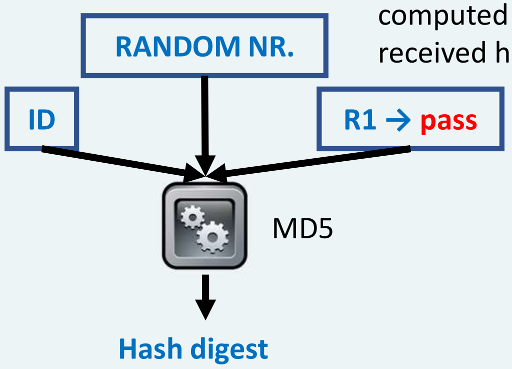
Responding CHAP


R1 responds to R3's CHAP challenge by sending its CHAP username and a hash value that is based on the CHAP password.

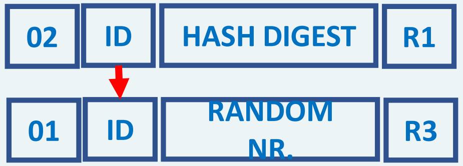
Source: Cisco CCNA; RFC 1994

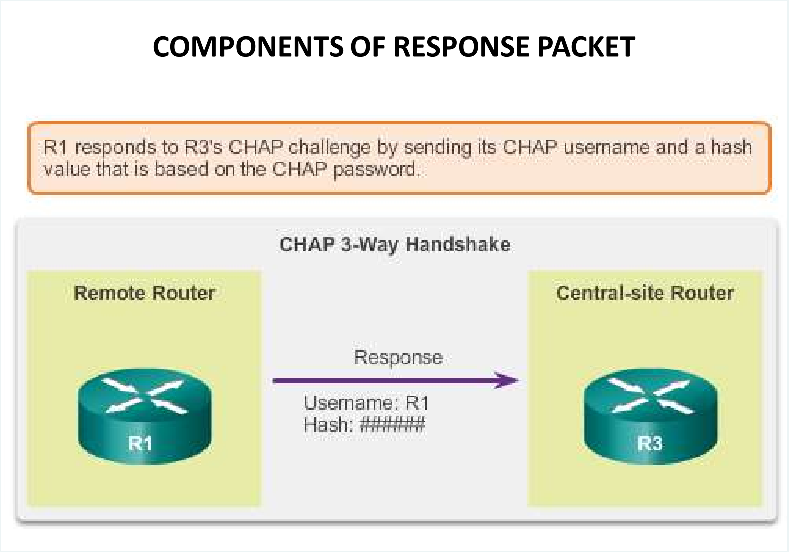
CHAP: Challenge Handshake Authentication Protocol

02	ID	HASH DIGEST	R1



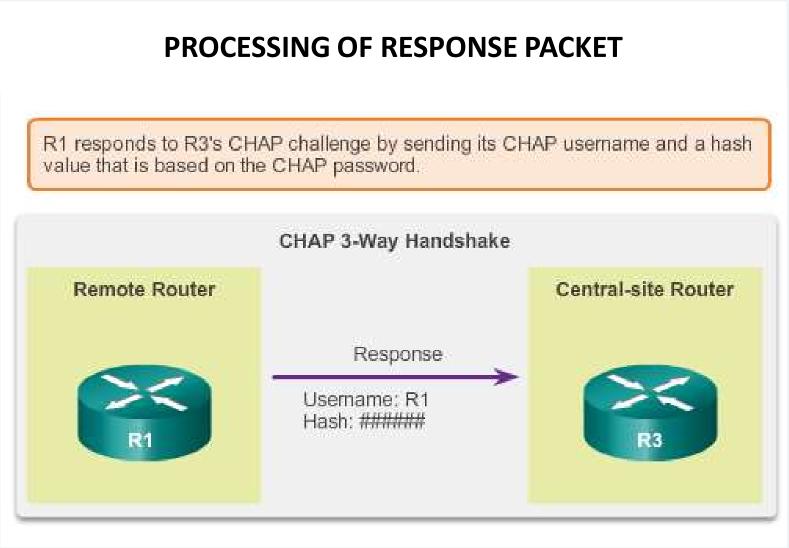
Comparison between computed hash digest & received hash digest





COMPONENTS OF RESPONSE PACKET

R1 responds to R3's CHAP challenge by sending its CHAP username and a hash value that is based on the CHAP password.

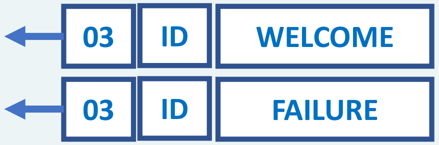


PROCESSING OF RESPONSE PACKET

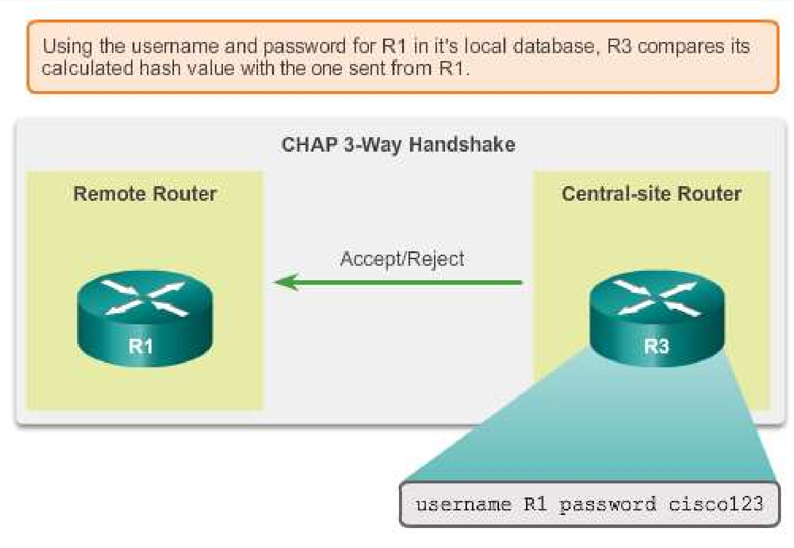
R1 responds to R3's CHAP challenge by sending its CHAP username and a hash value that is based on the CHAP password.

Source: Cisco CCNA

CHAP: Challenge Handshake Authentication Protocol (3)

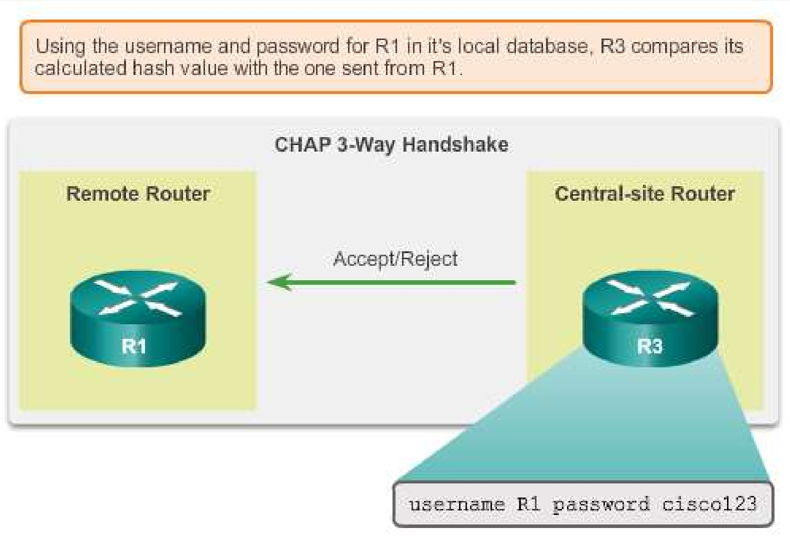


Completing CHAP


Using the username and password for R1 in it's local database, R3 compares its calculated hash value with the one sent from R1.

```
username R1 password cisco123
```

COMPONENTS OF AUTHENTICATION DECISION PACKET


Using the username and password for R1 in it's local database, R3 compares its calculated hash value with the one sent from R1.

```
username R1 password cisco123
```

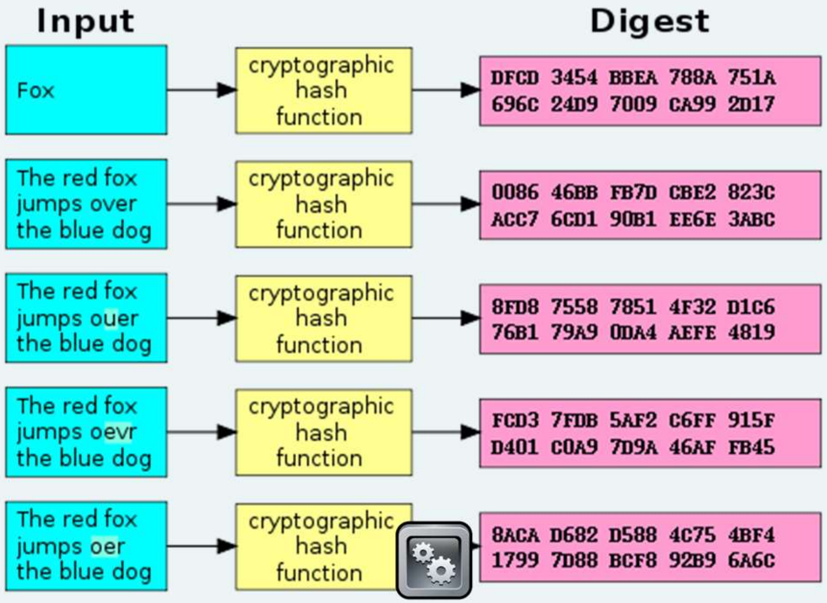
Source: Cisco CCNA

What can we say about the security provided by PPP?

- PAP provides little protection against impersonation
  - It is subject to eavesdropping
  - It is subject to replay attacks
  - It is subject to man in the middle attacks
- CHAP provides a higher level of protection
  - Due to the randomly-generated number used for the challenge and one-way hashing it is less vulnerable to replay attacks and eavesdropping
  - However, it suffers from similar weaknesses as symmetric encryption
    - We must both know the shared secret
    - We must communicate the shared secret out of band
    - If the shared secret is compromised, the protection is broken

Solution to message tampering: hashing

Changing a
single bit in
x will result
in a
different
value for *y*


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Idea behind hashing

For input data *x,* the output *y* is

$$y=h(x)$$

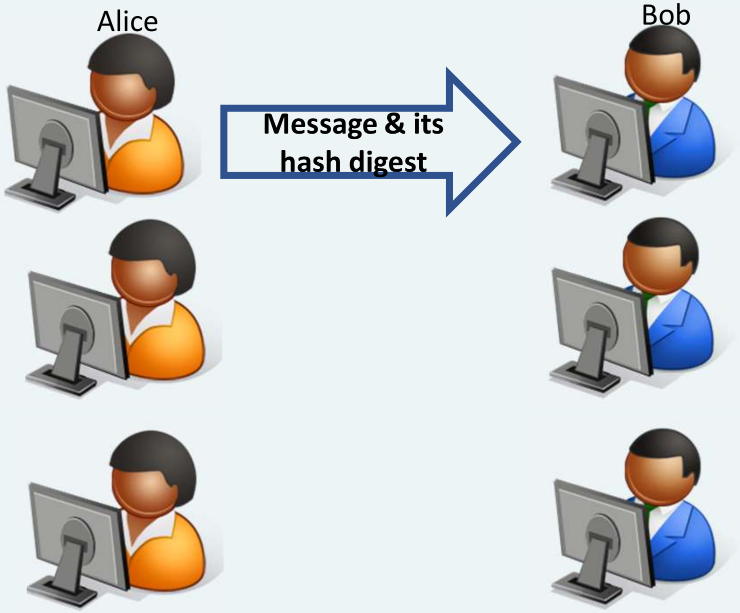
- Compression
  - Hashing algorithms produce a fixed size output of *y* regardless of the size of *x*. *y* is a fixed length, but needs to be ‘small’ for this to work
- Efficiency
  - The computation of *h(x)* should be efficient. It will grow for greater lengths of *x*, but shouldn’t take much longer
- One way
  - It should be difficult to invert the hash, i.e. Given *y* it should be difficult if not impossible to calculate *x*

Hashing algorithms

- Example hashing algorithms and digest size
  - MD5 hash algorithm produces 128-bits digests
  - SHA-1 hash algorithm produces 160-bits digests
  - SHA-256 hash algorithm produces 256-bits digests
  - SHA-512 hash algorithm produces 512-bits digests

…

Hashing in practice



1. Alice hashes a message with MD5 algorithm

2. Bob hashes the received message with MD5 algorithm

3. Bob compares the hash digest he computed with the one received from Alice
→ If they match: the message has not been tampered with

Potential problem with hashing: collision

- A collision happens when two different messages can be manipulated to generate a same hash digest
- A collision attack
  - on the MD5 hashing algorithm is known since 2004 (Wang et al. 2004)
  - on the SHA-1 hashing algorithm is known since 2005 (Wang et al. 2005)

MD5

- One way function (computationally infeasible to find correct input from output)
- Algorithm
  - produces 128 bit fixed length output
  - from 512bit block inputs
  - using 32 bit operations
  - Input padded to 512 bits using 10…0 until 64 bits left, then message length%2^^{64}

https://tools.ietf.org/html/rfc1321
https://en.wikipedia.org/wiki/MD5
http://merlot.usc.edu/csac-f06/papers/Wang05a.pdf

MD5

- ABCD are 32 bit words initialised to constants
- M_i is a 32 bit input block
- K_i is a 32 bit constant (different for each operation)
- This is performed 16 times for each of 4 different unique functions

$$F(B,C,D) = (B \wedge C) \vee (\neg B \wedge D)$$
$$G(B,C,D) = (B \wedge D) \vee (C \wedge \neg D)$$
$$H(B,C,D) = B \oplus C \oplus D$$
$$I(B,C,D) = C \oplus (B \vee \neg D)$$

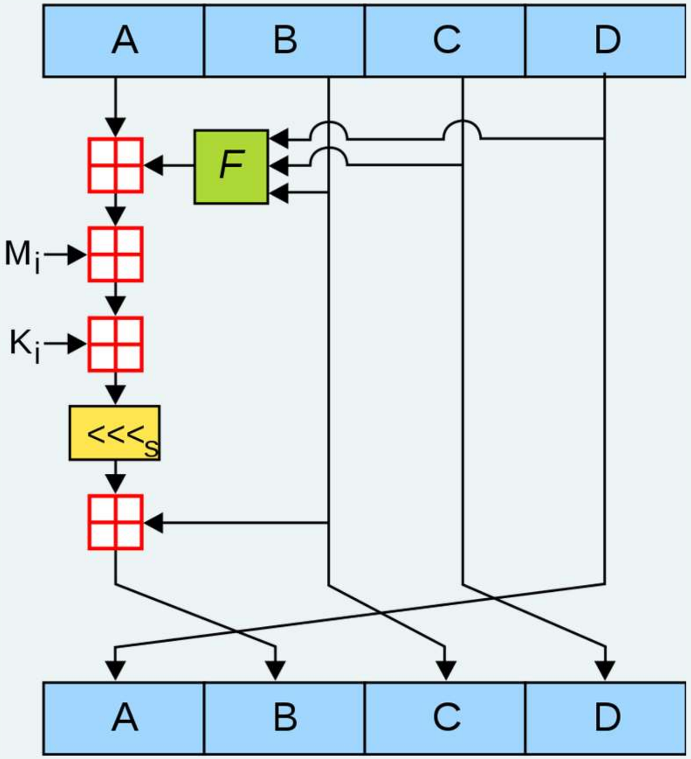
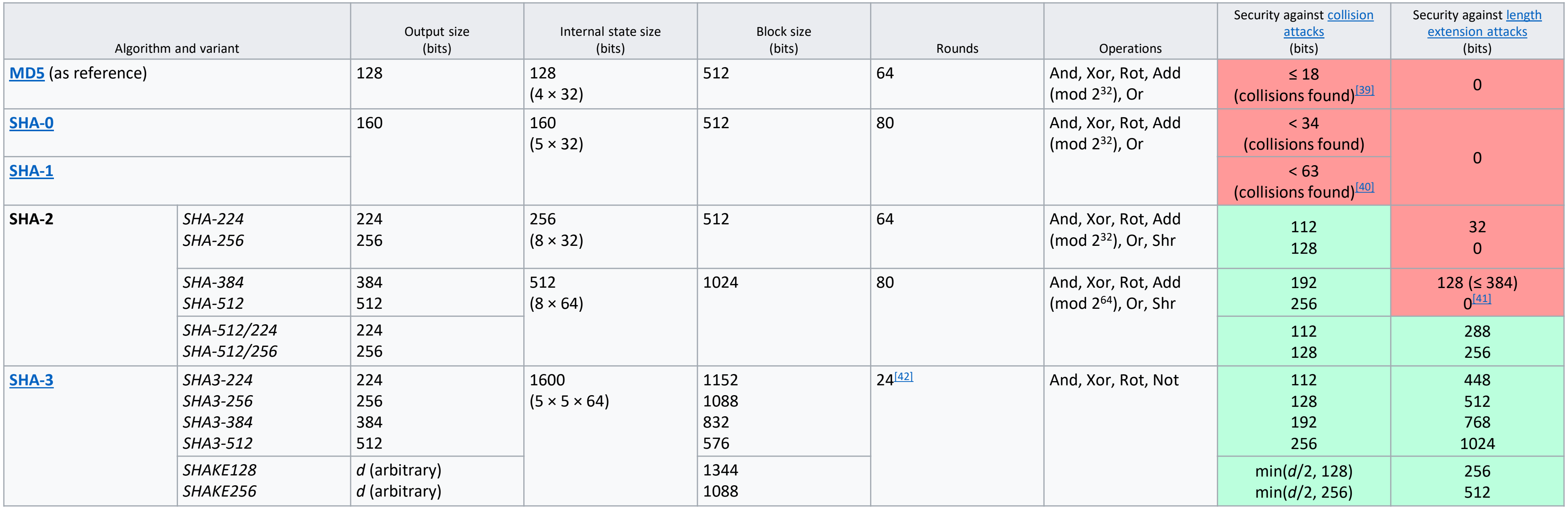


Figure 1. One MD5 operation. MD5 consists of 64 of these operations, grouped in four rounds of 16 operations. *F* is a nonlinear function; one function is used in each round. M_i denotes a 32-bit block of the message input, and K_i denotes a 32-bit constant, different for each operation. $<<<_s$ denotes a left bit rotation by *s* places; *s* varies for each operation. The red square with a cross denotes addition modulo 2^{32}.

SHA Family

- SHA-1 - Deprecated
- SHA-2 - In use, short versions are insecure
- SHA-3 - In use



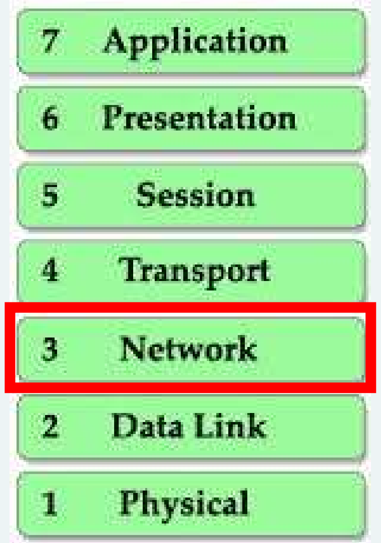
Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Rounds	Operations	Security against collision attacks (bits)	Security against length extension attacks (bits)
MD5 (as reference)		128	128 (4 × 32)	512	64	And, Xor, Rot, Add (mod 2^{32}), Or	≤ 18 (collisions found)[39]	0
SHA-0		160	160 (5 × 32)	512	80	And, Xor, Rot, Add (mod 2^{32}), Or	< 34 (collisions found)	0
SHA-1							< 63 (collisions found)[40]	
SHA-2	*SHA-224* *SHA-256*	224 256	256 (8 × 32)	512	64	And, Xor, Rot, Add (mod 2^{32}), Or, Shr	112 128	32 0
	SHA-384 *SHA-512*	384 512	512 (8 × 64)	1024	80	And, Xor, Rot, Add (mod 2^{64}), Or, Shr	192 256	128 (≤ 384) 0[41]
	SHA-512/224 *SHA-512/256*	224 256					112 128	288 256
SHA-3	*SHA3-224* *SHA3-256* *SHA3-384* *SHA3-512*	224 256 384 512	1600 (5 × 5 × 64)	1152 1088 832 576	24[42]	And, Xor, Rot, Not	112 128 192 256	448 512 768 1024

	SHAKE128
	SHAKE256
		d (arbitrary)
		d (arbitrary)
				1344
				1088
							min(*d*/2, 128)
							min(*d*/2, 256)
								256
								512

IPSec Protocol

- Provides security for IPv4 and IPv6 packets, allowing secure remote communication over the Internet
- Three main technologies:
  - Authentication Headers
    - data integrity, data origin authentication, replay attack prevention
  - Encapsulating Security Payloads
    - Confidentiality, data origin authentication, integrity, replay attack prevention
  - Security Associations
    - Key exchange and location services
- Can be used by any higher layer protocol

(Main reference: RFC 2401)

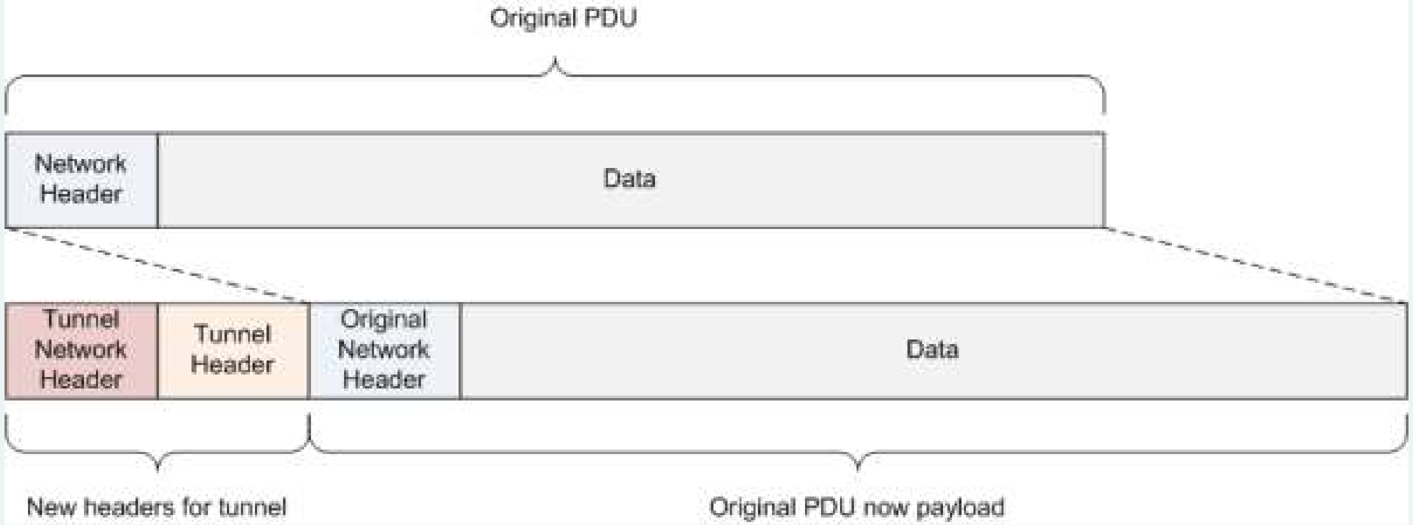


https://en.wikipedia.org/wiki/IPsec

IPSec: Transport Mode

- Encrypts the payload only
- Breaks with port / network address translation
  - Hash is different so packet is market as tampered with
  - NAT-T protocol allows for NAT and IPSec
- Security protocols:
  - https://tools.ietf.org/html/rfc7321
  - HMAC- SHA1, SHA2 – integrity, protection, authenticity
  - TripleDES-CBC – confidentiality
  - AES-CBC – confidentiality
  - AES-GCM confidentiality, authentication

IPSec: Tunneling Mode

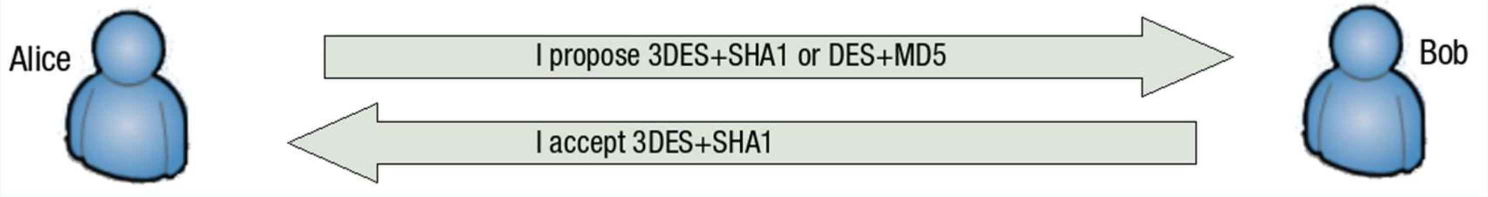


Source: http://infrastructureadventures.com/tag/ipsec/

Sensitivity: Internal

Internet Key Exchange (IKE) service

- IKE is used to encrypt IPSec packets
- In IKE (RFC 2409), the pair of hash and encryption algorithms is negotiable
- Decision depends on security policy of end points



http://documentation.axsguard.net/manuals/Gatekeeper/7.7.0PL2/html/ipsec/

- You will need to implement something like this for your second practical
- Negotiation of encryption and authentication is an important factor for future proofing your protocol

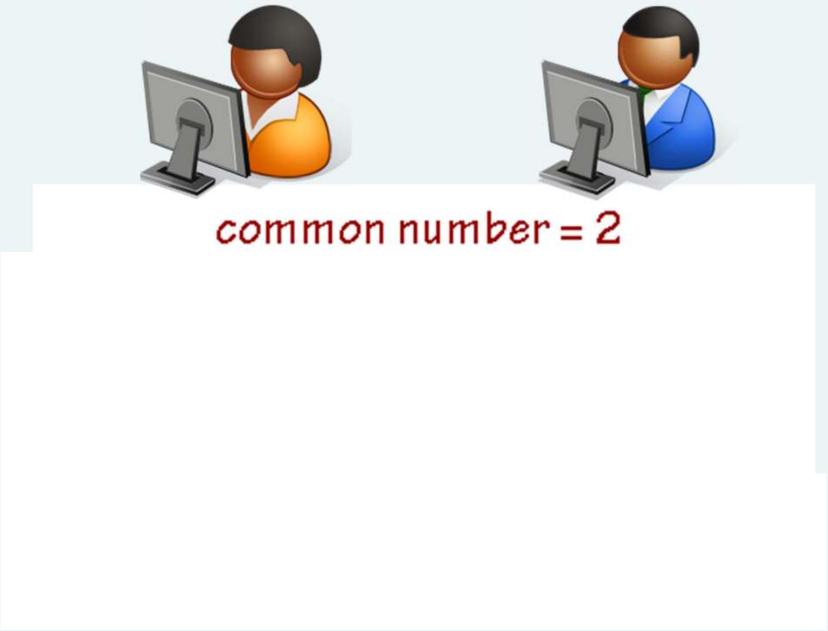
Internet Key Exchange

- IKEv1:
  - symmetric encryption, shared secret key
  - asymmetric encryption
    - public key encryption and digital signature
  - Many problems with difficult to interpret output and very strict negotiations
- IKEv2
  - Allows mobility (MOBIKE), NAT, increased DOS resilience (less forward processing)
- For symmetric encryption
  - enforces periodic secret key change and frequent refresh
  - administrator can control key strength and refresh frequency

http://www.ciscopress.com/articles/article.asp?p=25474&seqNum=7

https://en.wikipedia.org/wiki/Internet_Key_Exchange

IPSec uses Diffie-Hellman key exchange method



Shared key is never transmitted

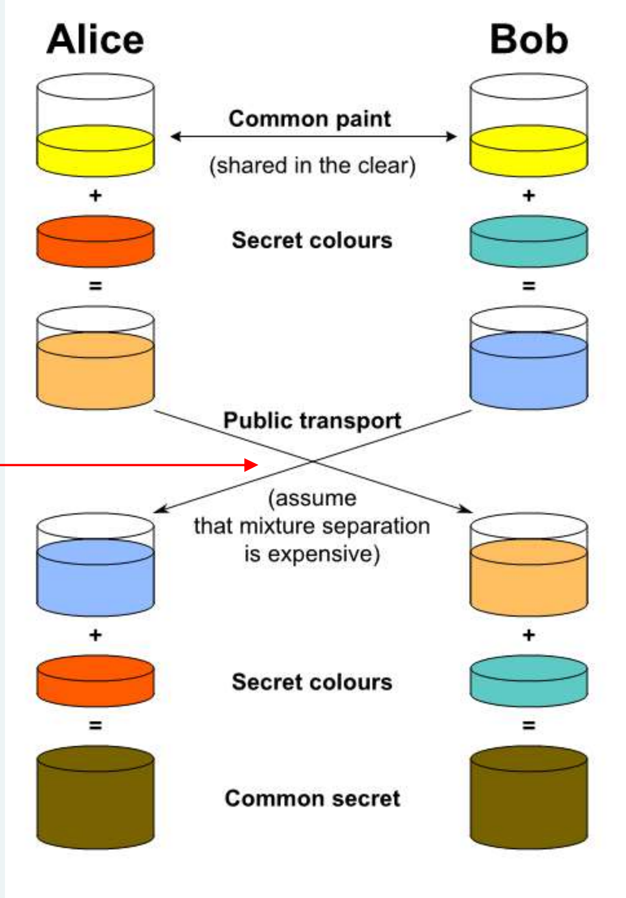
https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

Why does it work

1. Alice and Bob agree to use a modulus p = 23 and base g = 5 (which is a primitive root modulo 23).
2. Alice chooses a secret integer $\boldsymbol{a}$ = 4, then sends Bob $A = g^{a}$ mod p
   - $A = 5^{4}$ mod 23 = 4
3. Bob chooses a secret integer $\boldsymbol{b}$ = 3, then sends Alice $B = g^{b}$ mod p
   - $B = 5^{3}$ mod 23 = 10
4. Alice computes $\boldsymbol{s} = B^{a}$ mod p
   - $\boldsymbol{s} = 10^{4}$ mod 23 = 18
5. Bob computes $\boldsymbol{s} = A^{b}$ mod p
   - $\boldsymbol{s} = 4^{3}$ mod 23 = 18
6. Alice and Bob now share a secret (the number 18).
7. Both Alice and Bob have arrived at the same value s, because, under mod p,

$$(g^{a} mod\ p)^{b} \text{mod p} = (g^{b} mod\ p)^{a} \text{mod p}$$

This is the key – its difficult to determine the prime number if we use a really big number!



Sensitivity: Internal

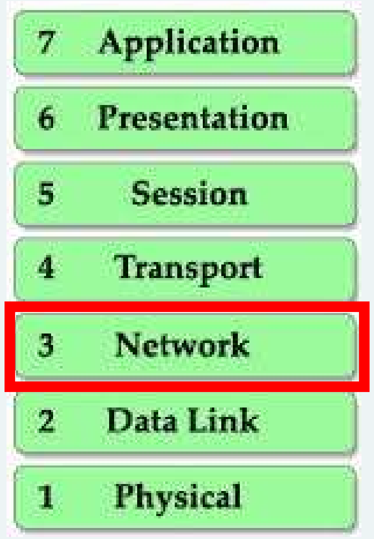
What can we say about the security provided by IPSec?

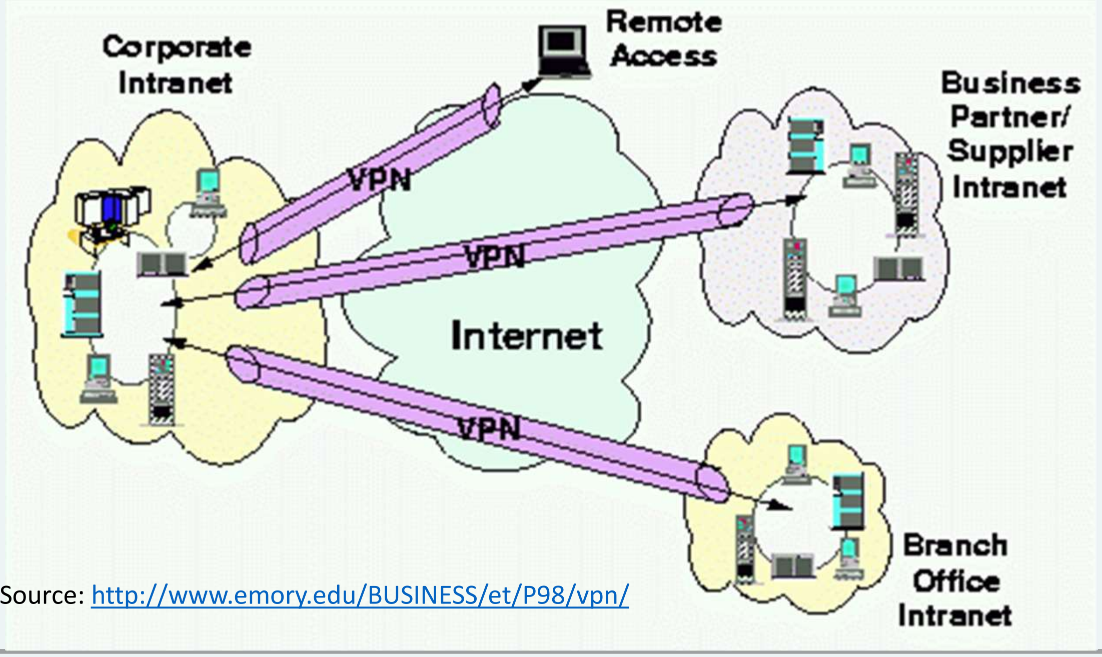
- IPSec provides several mechanisms to ensure confidentiality, integrity and authentication
- Basically
  - IPSec encrypts
  - then authenticates
  - then tunnels/encapsulates a packet before transmission
- IPSec is not mandatory but is useful for security and providing things like VPN services.

https://www.geeksforgeeks.org/ip-security-ipsec/ Is a very nice description of IPSec

Virtual Private Network – VPN

- Uses the Internet as the public backbone for access to a secure private network → it extends the private network





Source: http://www.emory.edu/BUSINESS/et/P98/vpn/

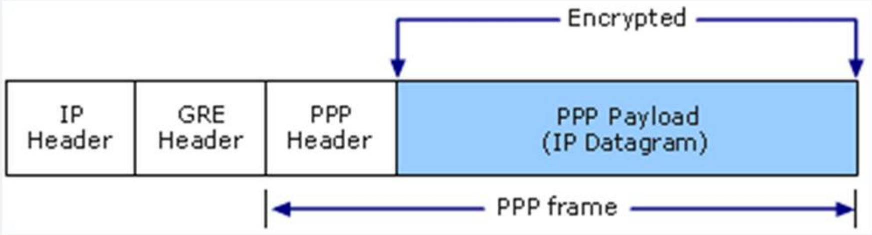
VPN tunneling

- VPN can be implemented via tunnelling protocols such as
  - PPTP (Point-to-Point Tunneling Protocol) – largely obsolete
    - https://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol
  - L2TP (Layer Two Tunneling Protocol)
    - https://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol
  - SSTP (Secure Socket Tunneling Protocol)
    - https://en.wikipedia.org/wiki/Secure_Socket_Tunneling_Protocol

- All of those depend on features of the Point to Point Protocol (PPP)

PPTP

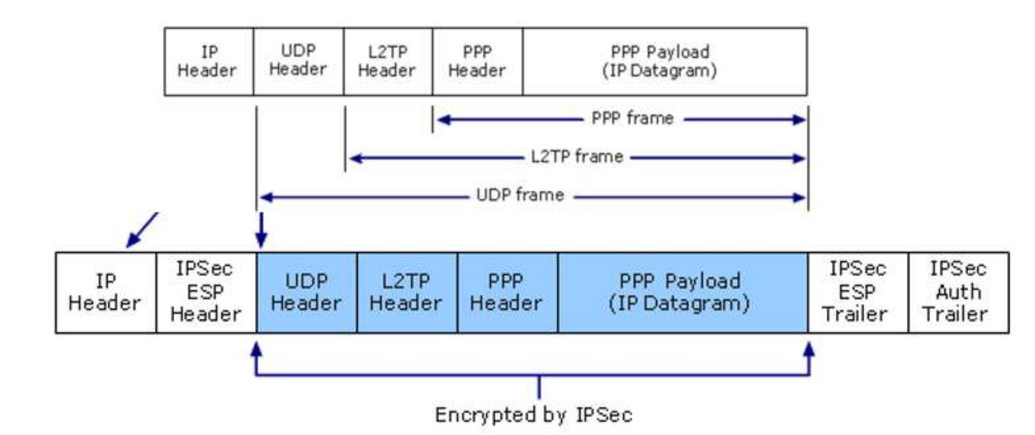
- PPTP encapsulates PPP frames in IP datagrams
  - PPTP does not provide encryption or authentication
  - Authentication can be done using PAP or CHAP (or EAP for wireless)
  - Obsolete and with security flaws
  - Essentially:
    - Wraps the PPP content with a new header
    - Receiving end unwraps and performs appropriate actions on the payload



Source: http://technet.microsoft.com/en-us/library/cc771298%28v=ws.10%29.aspx https://tools.ietf.org/html/rfc2637

L2TP

- L2TP is a combination of PPTP & Layer 2 Forwarding (L2F), developed by Cisco
  - L2TP relies on Internet Protocol security (IPsec) for encryption services
    - https://tools.ietf.org/html/rfc3193



Source: http://technet.microsoft.com/en-us/library/cc771298%28v=ws.10%29.aspx

https://tools.ietf.org/html/rfc2661

SSTP

- Tunneling protocol that uses the HTTPS protocol to pass traffic through firewalls and Web proxies that might block PPTP and L2TP/IPsec traffic
  - The SSTP message is encrypted with the SSL channel of HTTPS
  - OpenVPN and SoftEther VPN use SSTP

VPN – security features

- Confidentiality
  - PPTP, L2TP/IPSec and SSTP protocol suites provide confidentiality via encryption
- Integrity and Authentication
  - L2TP/IPSec provides authentication via IPSec – asymmetric or symmetric-based authentication
  - SSTP provides integrity and authentication inherited from SSL
  - PPTP does not provide features to assure data integrity or protection against impersonation

Further Reading:

- Network security essentials, 6th edition. William Stallings, Pearson
- *Computer Networking: A Top Down Approach* , 7th edition. Jim Kurose and Keith Ross. Addison-Wesley.
- Security in Computing, 5th edition. Charles P. Pfleeger and Shari L. Pfleeger. Pearson Education.
- Reading:
  - http://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.html
  - http://technet.microsoft.com/en-us/library/bb742596.aspx
  - https://www.infosec.gov.hk/english/technical/files/vpn.pdf
- Video:
  - Network Security 101: https://www.youtube.com/watch?v=E03gh1huvW4
  - Cyber Security in 7 minutes: https://www.youtube.com/watch?v=inWWhr5tnEA
  - Computerphile Networking and Security playlist: https://www.youtube.com/watch?v=PG9oKZdFb7w&list=PLt6GfwFEfTfNPsY4kfLnEe6niP4qECxkX

UNIVERSITY OF DERBY

University of Derby, Kedleston Road, Derby, DE22 1GB
T +44 (0)1332 591044 **E** opendays@derby.ac.uk

THANK YOU

derby.ac.uk

Sensitivity: Internal