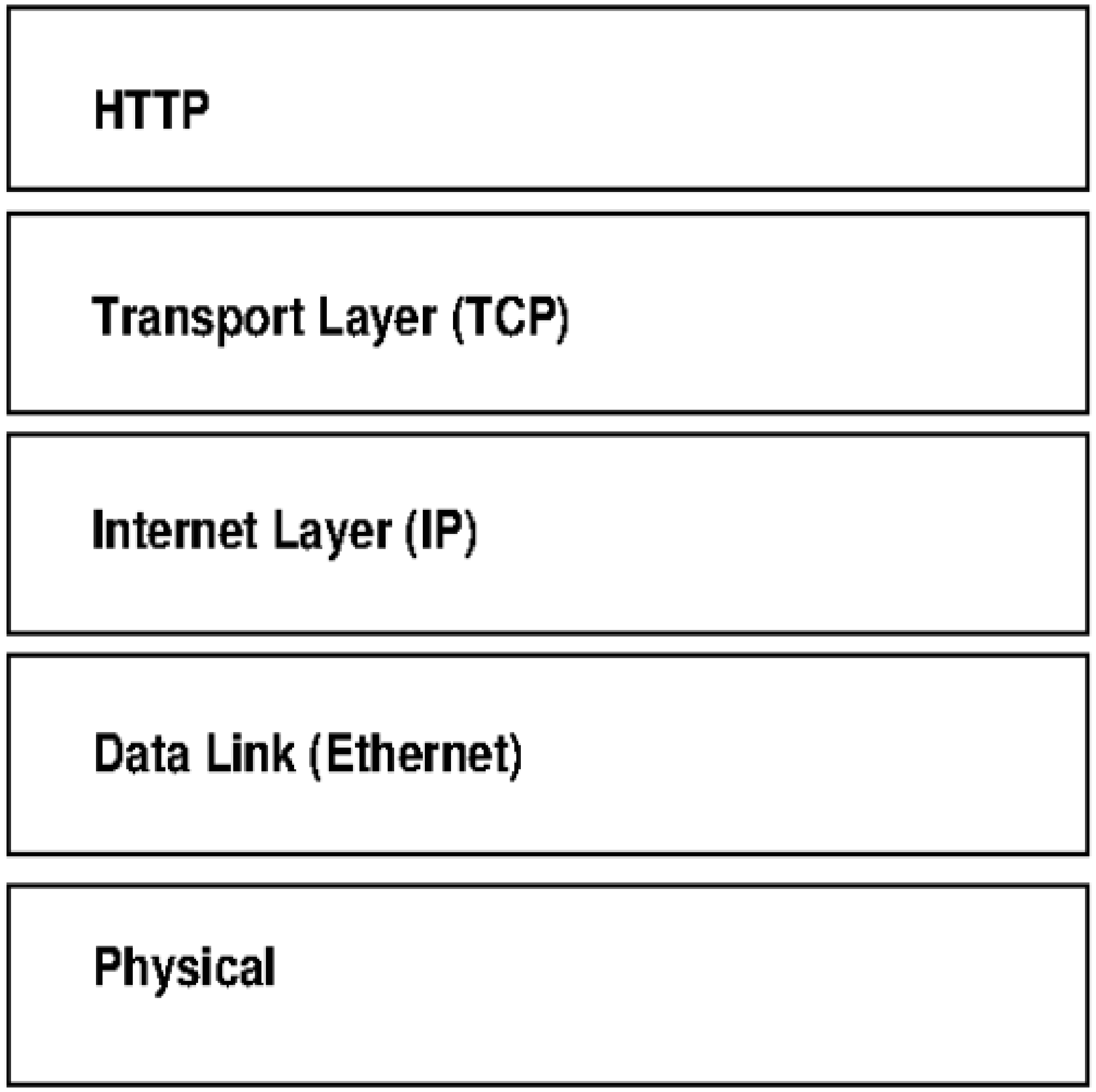
FIT 1047

Introduction to computer systems, networks and security

MONASH University

Security Protocols

Network Stack with HTTP



HTTP

Transport Layer (TCP)

Internet Layer (IP)

Data Link (Ethernet)

Physical

Security above Transport Layer - TLS

Security above Transport Layer - TLS

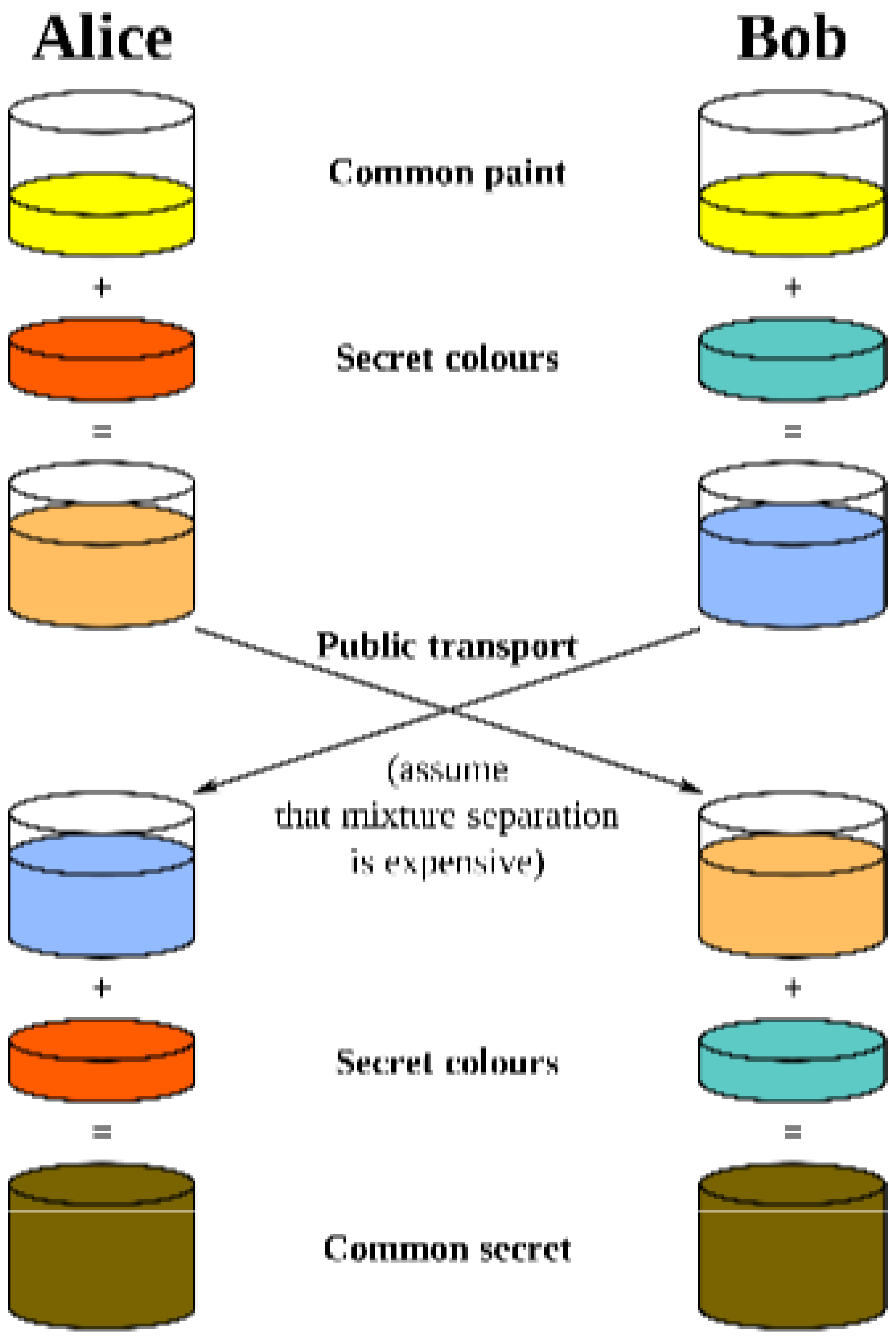
SSL/TLS

- Originally developed by Netscape as Secure Socket Layer SSL
- SSL Version 2.0 in 1995 was quickly replaced by SSL 3.0 in 1996
- IETF (Internet Engineering Taskforce) published successor Transport Layer Security 1.0 as RFC5246 in 1999
- Current version is TSL 1.2 as IETF RFC 5246
- All previous versions should be disabled due to security problems.

SSL/TLS

- Main goal is to establish a shared key to protect messages (confidentiality and integrity/authenticity)
- Main sub-protocols are TLS handshake to negotiate parameters, optional authentication, establish shared key
- and TSL record, which is the actual secure transport protocol
- Uses Diffie-Hellman key exchange to create the shared secret

Diffie-Hellman key exchange



(Wikipedia)

Diffie-Hellman key exchange

1. Alice and Bob agree on a value g (these values are public)

2a. Alice generates random A and a=g^A

2b. Bob generates a random B and b=g^B

3. They exchange a and b

4. Shared key is K= b^A = g^{BA} = g^{AB} = a^B

Why does this work?

A and B are secret values.

$a=g^A$ and $b=g^B$ are public

To get A or B, the attacker would need to compute A from g^A

This discrete logarithm is difficult to compute!

TLS Phases

1. TLS Handshake

Can authenticate server and client. In HTTPS mostly only the server is authenticated. Results in a shared key and session ID or session ticket.

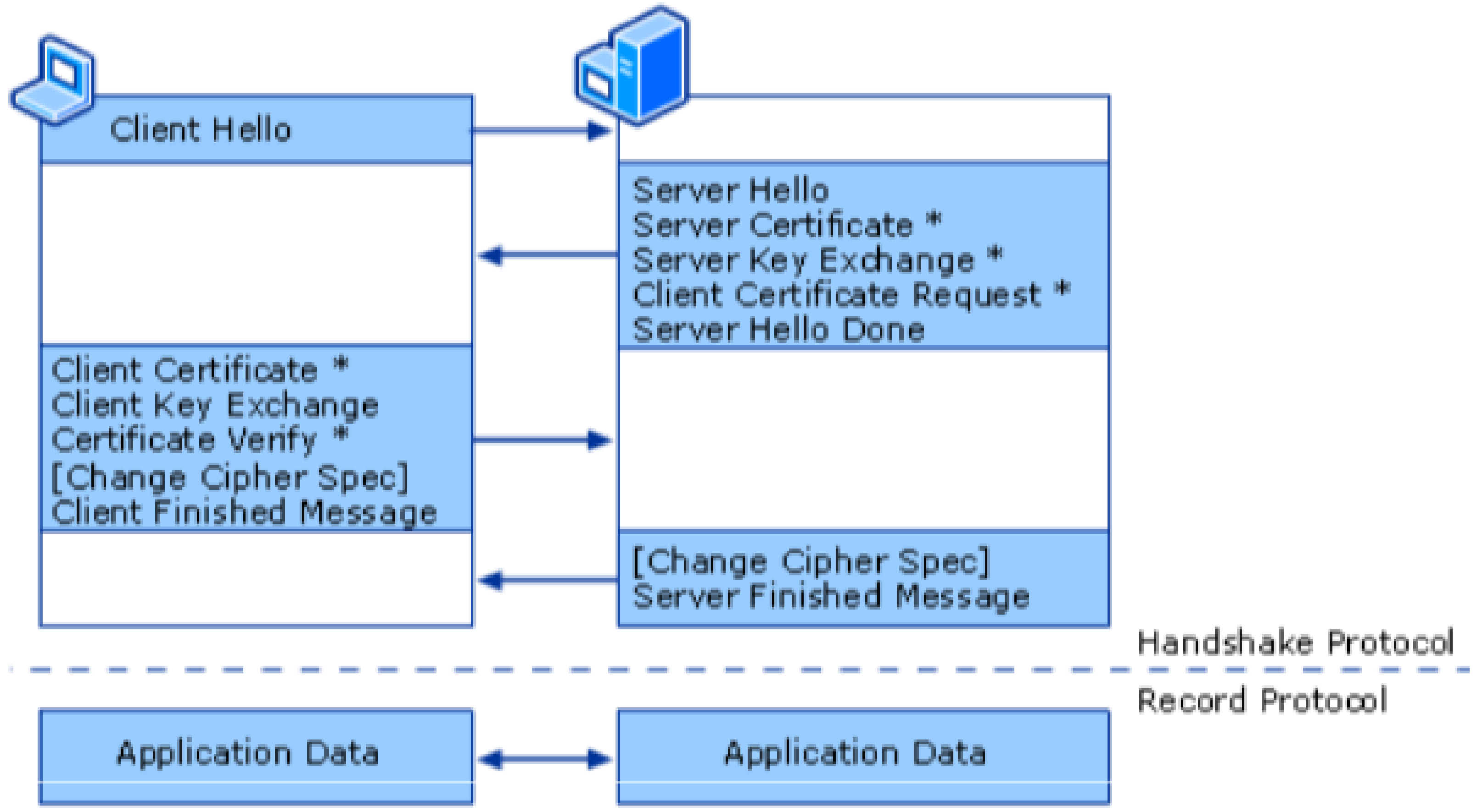
1. TLS Record

After the exchange of ChangeCipherSpec messages, all subsequent traffic is encrypted.

1. TLS Alert

Immediately closes a session

A closer look at TLS Handshake



Client Hello

Server Hello
Server Certificate *
Server Key Exchange *
Client Certificate Request *
Server Hello Done

Client Certificate *
Client Key Exchange
Certificate Verify *
[Change Cipher Spec]
Client Finished Message

[Change Cipher Spec]
Server Finished Message

Handshake Protocol

Record Protocol

Application Data

Application Data

* Optional or situation-dependent messages

[Change Cipher Spec] is not a TLS handshake message but is an independent, TLS Protocol content type that helps the parties avoid a pipeline stall.

(Source: Microsoft)

Authentication with certificates

- A certificate provides additional information for a public key.
- Owner of the matching private key
- Validity (expiration date and time)
- Subject name
- Issuer name
- other parameters

Trusted certificates

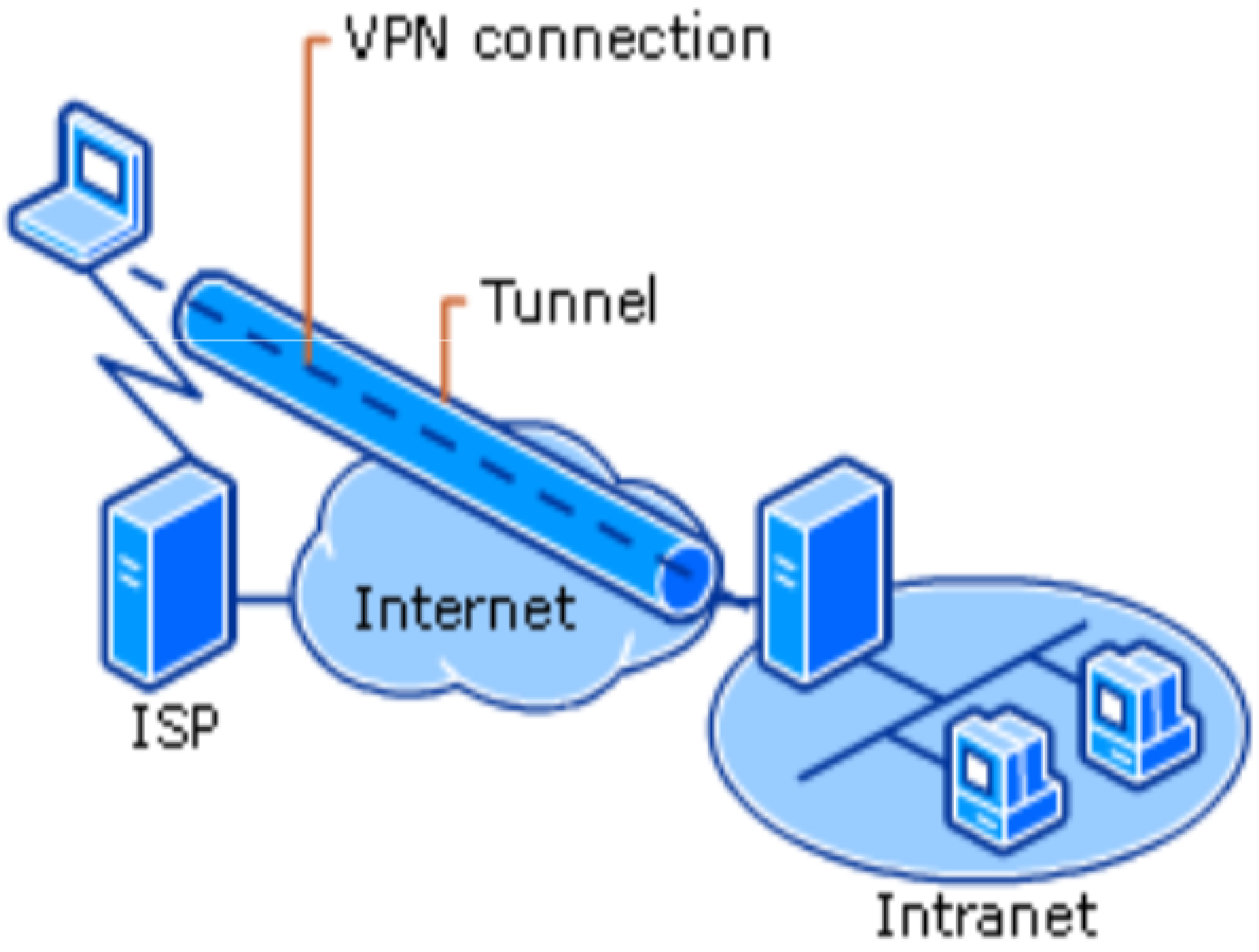
- A trusted certificate is digitally singed by a known certification authority
- Browsers (Chrome, Firefox, IE, Safari, etc.) come with a list of these authorities.

Certificates have problems

- Certificate revocation
- Relation between name and principal
- Users are used to accept certificates with errors
- New policies are stricter (which sometimes is annoying)

VPN - Virtual Private Network

- A VPN logically connects a client (or a network) to a network via an encrypted channel.



(Source: Microsoft)

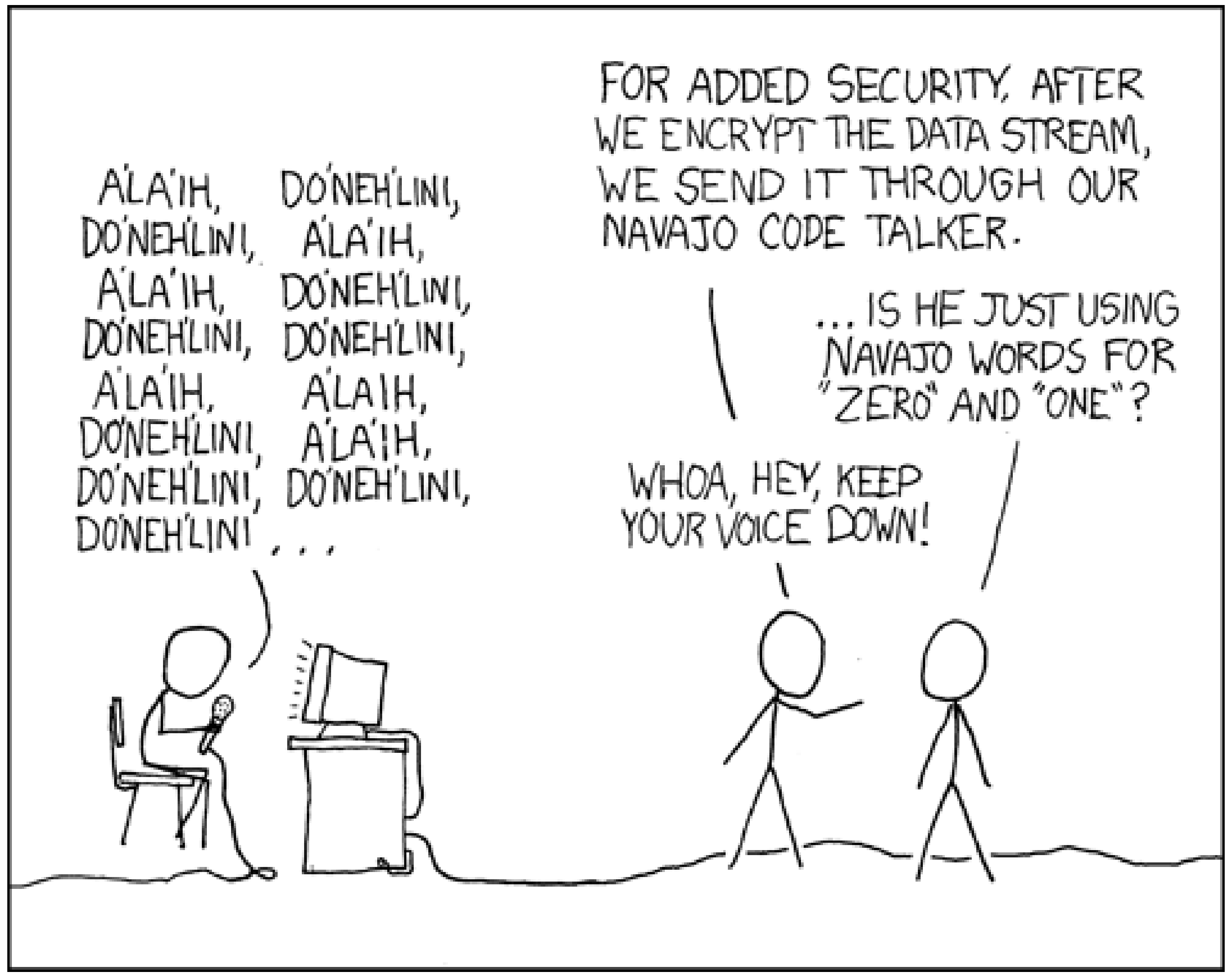
- A VPN routes packet between different networks.
- Tunnel can be established by TLS, IPSec
- Security only between tunnel endpoints, e.g. VPN client and VPN gateway. Traffic in an internal network is still in clear!

IPSec

A protocol suite on the level of IP packets:

- Can authenticate and encrypt data for each IP packet of a communication
- Transport mode: Payload in IP packets is encrypted, integrity of header is protected. used for example for end-to-end communication between two devices.
- Tunneling mode: Complete IP packets are encrypted and contained in a new IP packet with a new header. Used for VPNs and host-to-host/network-to-network communication.

Not all additional cryptography improves security



A'LA'IH, DO'NEH'LINI, DO'NEH'LINI, A'LA'IH, A'LA'IH, DO'NEH'LINI, DO'NEH'LINI, DO'NEH'LINI, A'LA'IH, A'LAIH, DO'NEH'LINI, A'LA'IH, DO'NEH'LINI, DO'NEH'LINI, DO'NEH'LINI . . .
FOR ADDED SECURITY, AFTER WE ENCRYPT THE DATA STREAM, WE SEND IT THROUGH OUR NAVAJO CODE TALKER.
... IS HE JUST USING NAVAJO WORDS FOR "ZERO" AND "ONE"?
WHOA, HEY, KEEP YOUR VOICE DOWN!

(xkcd.org)

For explanations look here:
https://www.explainxkcd.com/wiki/index.php/257:_Code_Talkers