FIT 2093

Introduction to cyber security

MONASH University

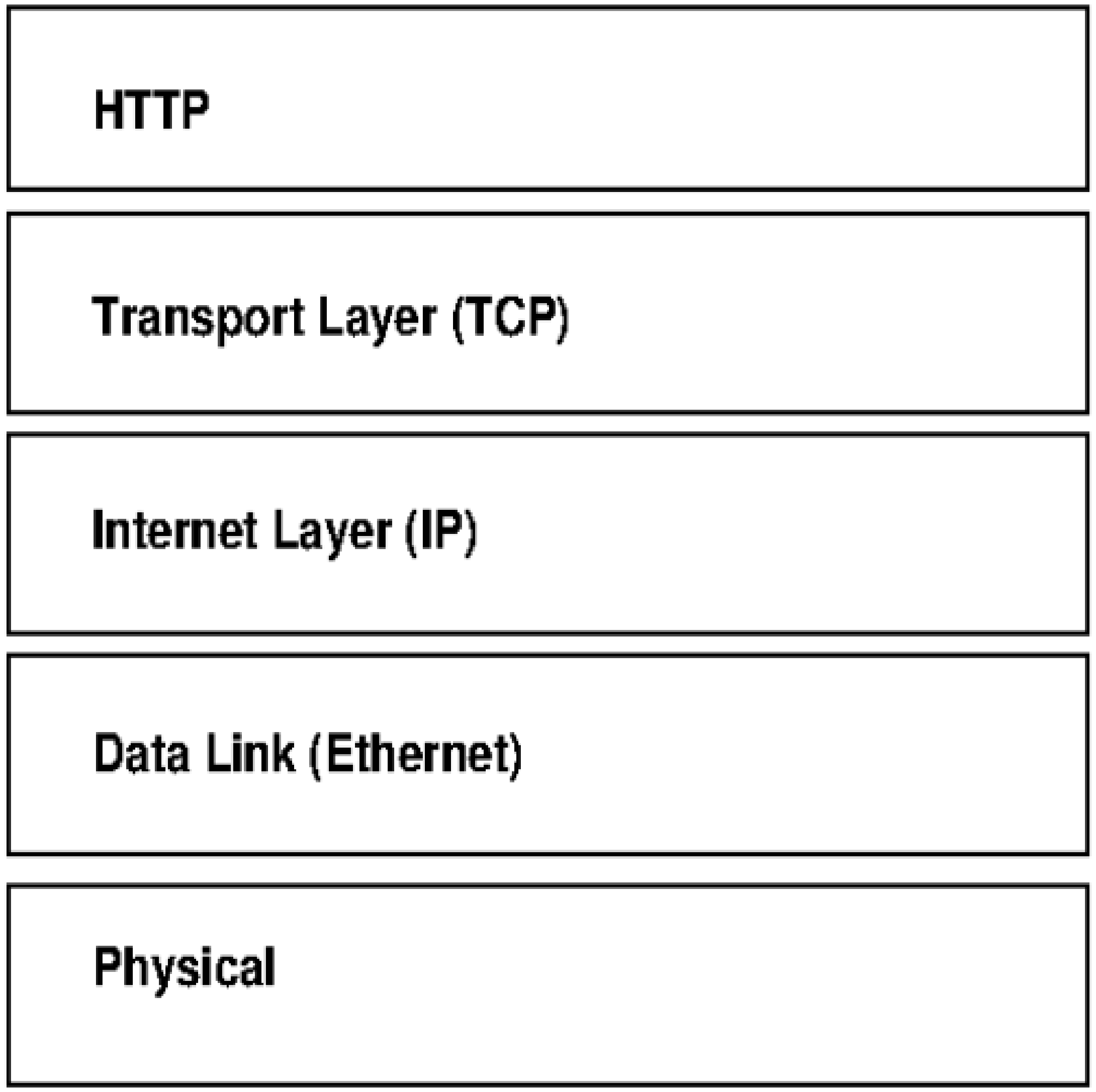
Space	Forward
Right, Down, Page Down	Next slide
Left, Up, Page Up	Previous slide
P	Open presenter console
H	Toggle this help

Some aspects of practical security

- Protocols
- TLS / HTTPS
- VPNs
- Firewalls
- Deep Packet Inspections, Intrusion Prevention

Space	Forward
Right, Down, Page Down	Next slide
Left, Up, Page Up	Previous slide
P	Open presenter console
H	Toggle this help

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

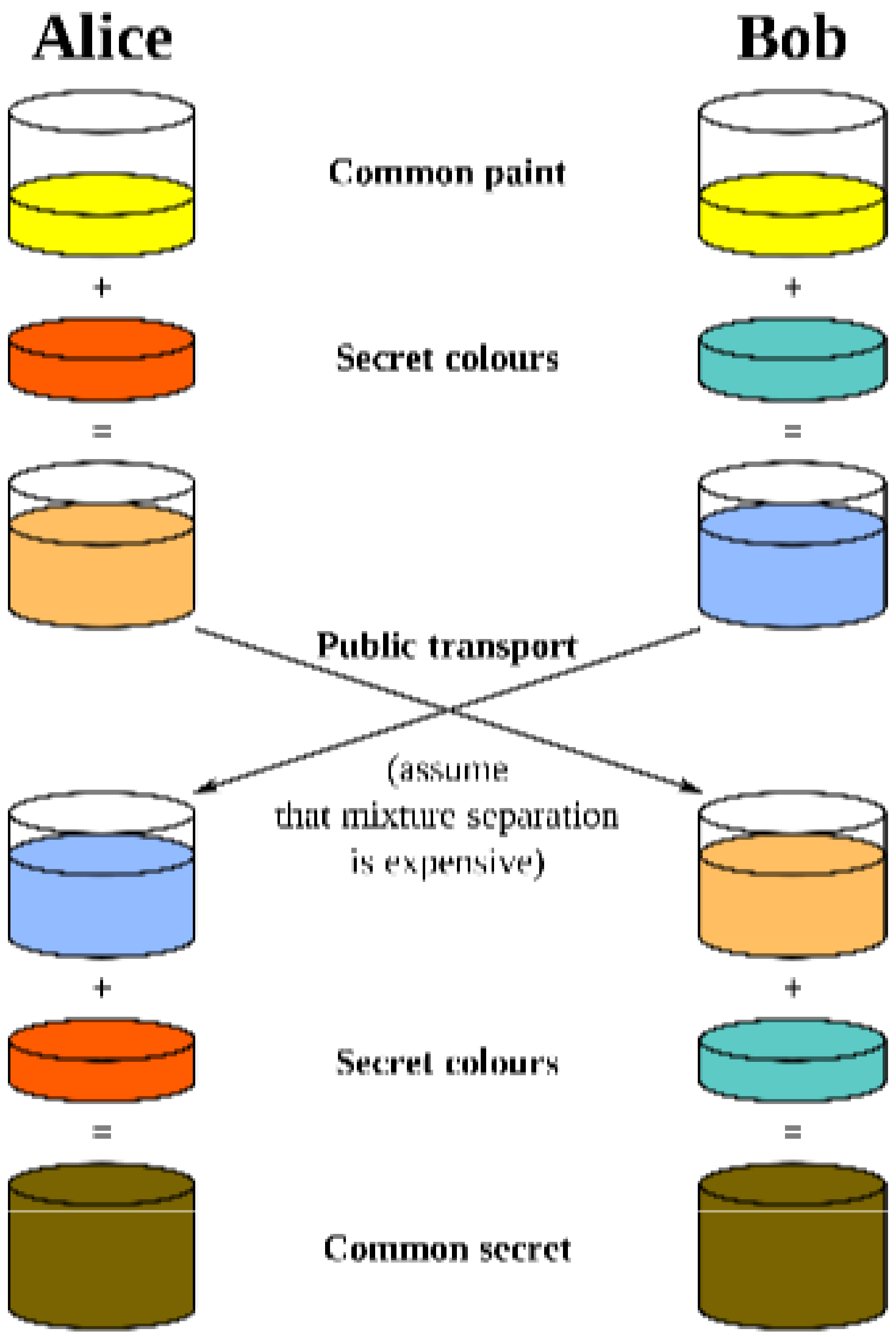
SSL/TLS

- 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 TLS 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 base g and modulus n (these values are public)

2a. Alice generates random A and $a=g^A$ mod n

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

3. They exchange a and b

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

[illegible]

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.

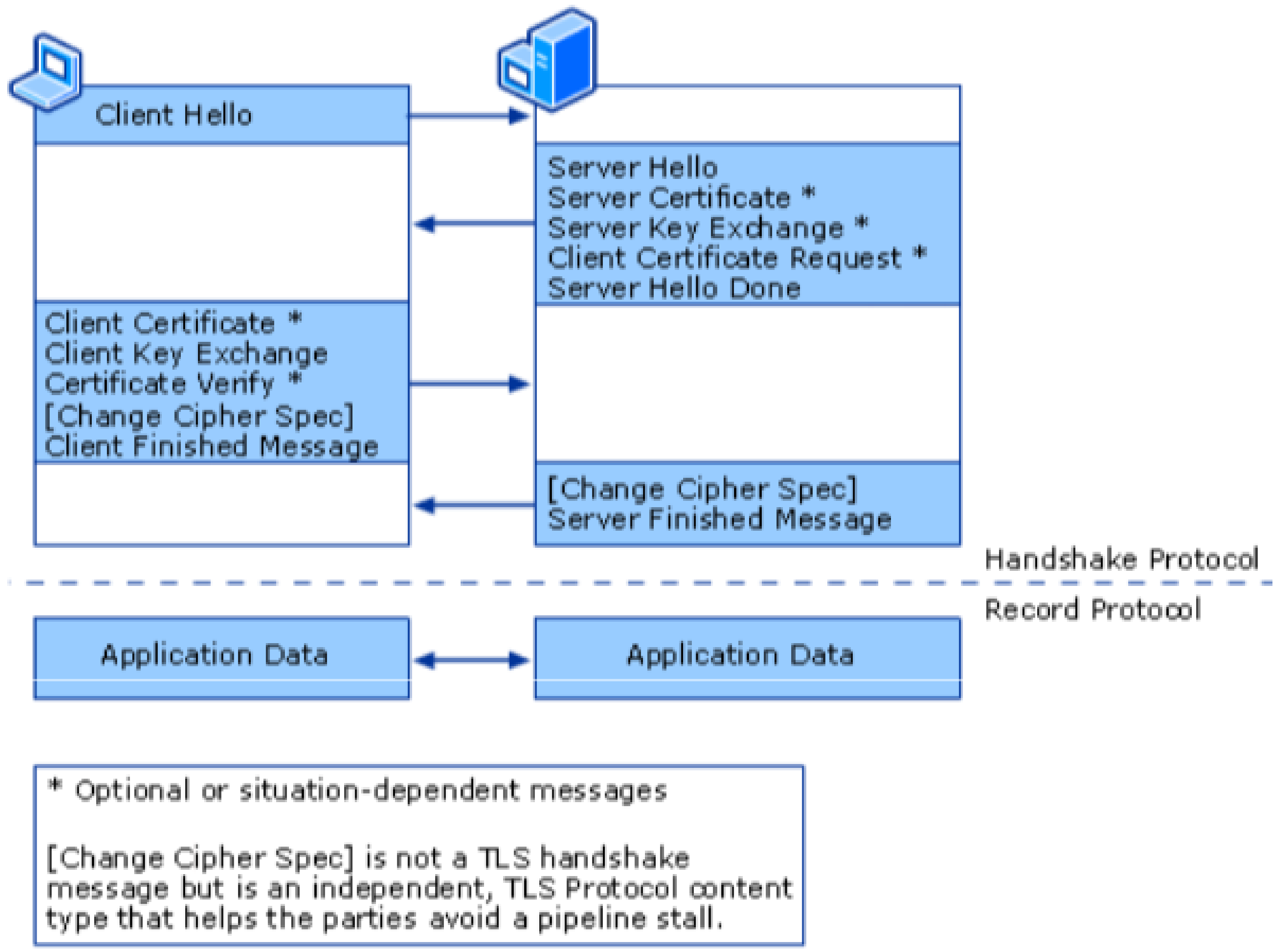
1. TLS Record

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

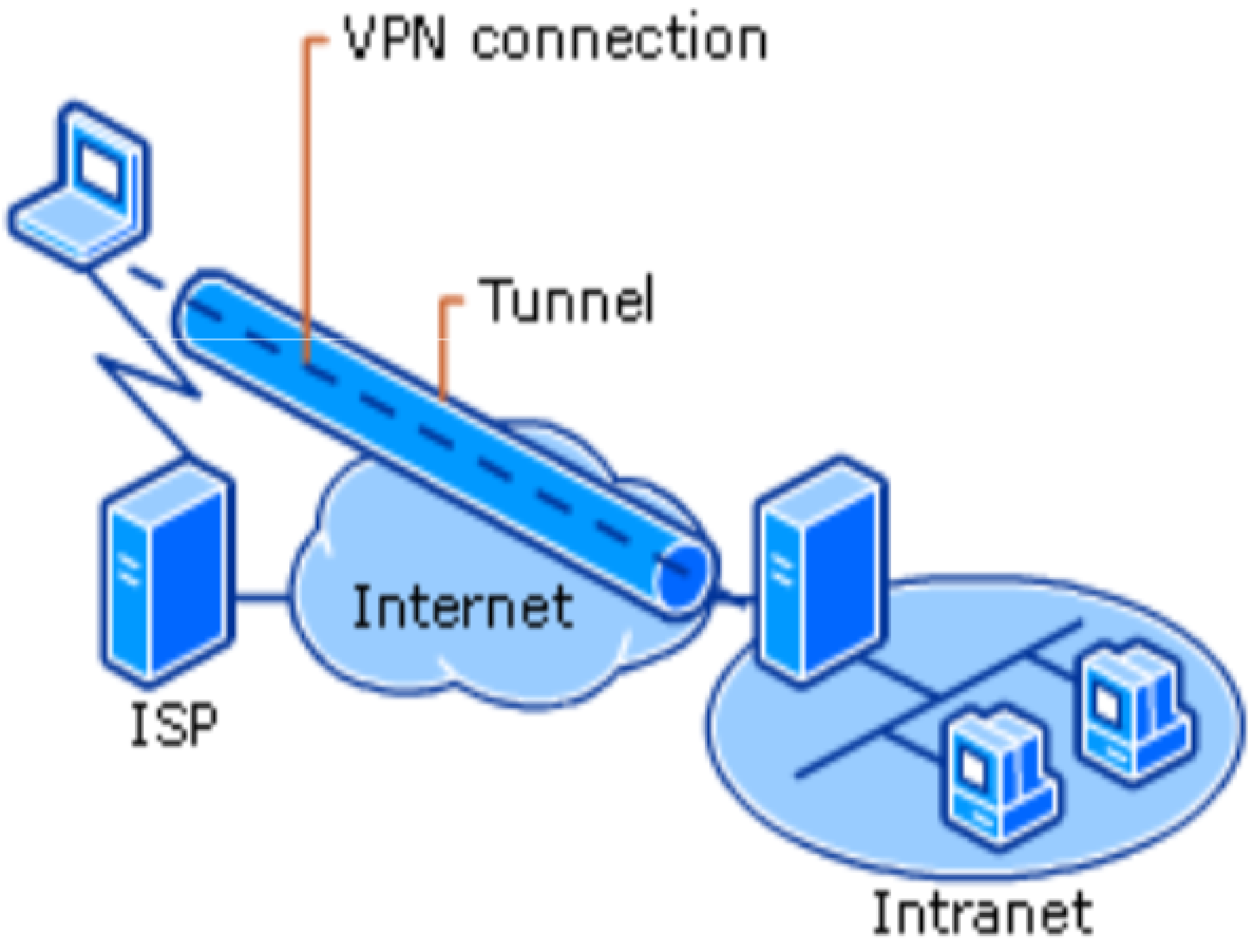
- A trusted certificate is digitally singed by a known certification authority
- Browsers (Chrome, Firefox, IE, Safari, etc.) come with a list of these authorities.

Certificates have problems

- Certificate revocation
- Relation between name and principal
- In the past, very often users hat to accept certificates with errors
- This has improved and new policies are stricter (which sometimes can be 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.

IPSec Core Protocols

AH Authentication Header: provides connectionless integrity and data origin authentication. IETF RFCs for a number of options: Keyed SHA1, different HMACs

ESP Encapsulating Security Payload main goal is confidentiality, but can also provide authentication, integrity, some kind of anti-replay and limited traffic flow integrity. Mostly uses AES in GCM or CCM, but other algorithms are also defined.

IPSec Authentication

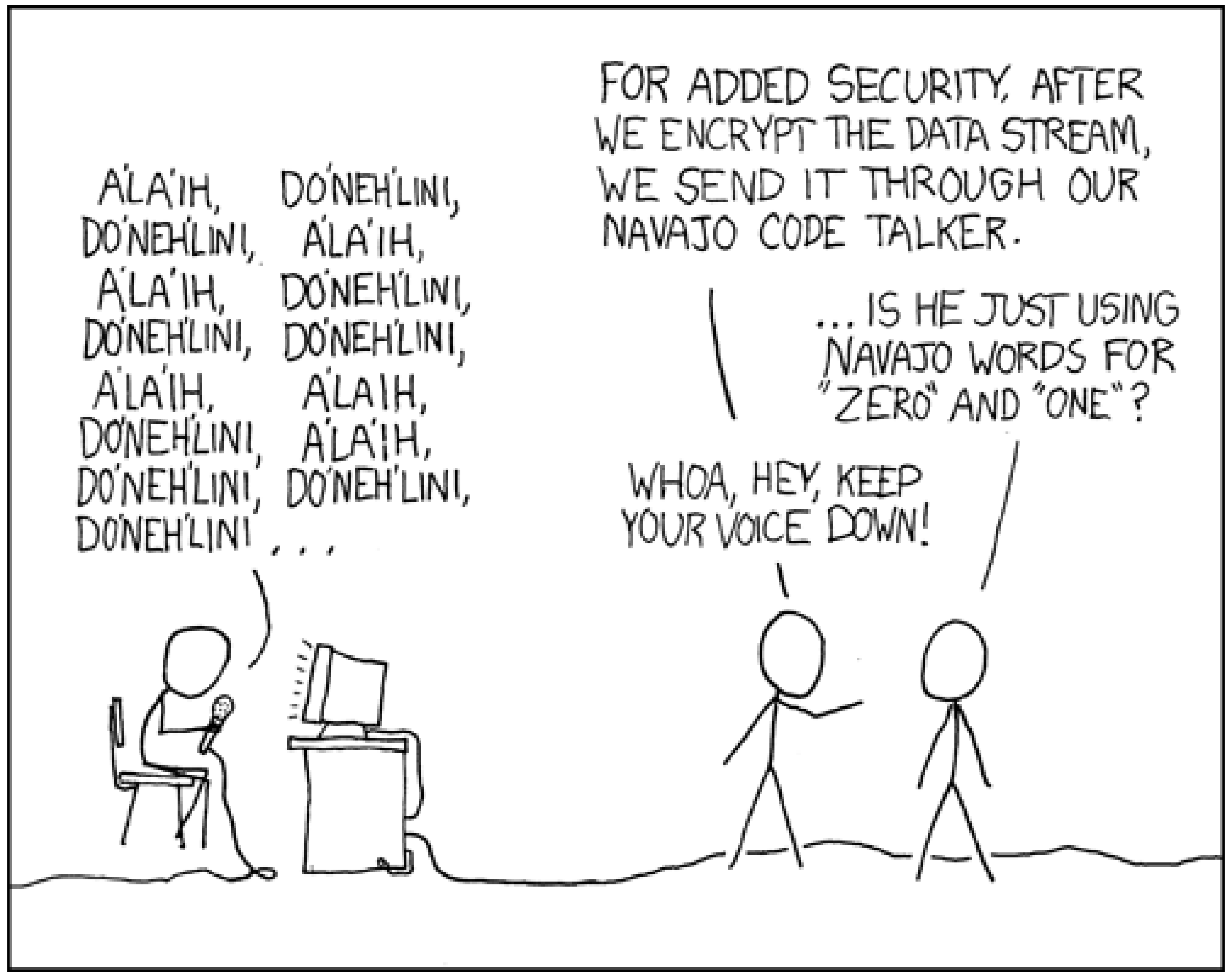
- Before AH or ESP can be used, keys need to be established. (security association)
- IKE Internet Key Exchange is used for this.
- IKE can use pre-shared keys or certificates.

Protecting Keys

An alternative way to establish security associations:

- Use a Trusted Platform Module TPM to generate and protect keys.
- Provides a secure device identity.
- TLS and IKE can both use TPM-based authentication.

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

Overview for the next section

- Firewalls
- Network View on Firewalls - Perimeter Protection
- DMZ - demilitarized zone
- Next generation firewalls
- Virus scanner

What is a Firewall?

Firewall

- A firewall is some kind of barrier
- In computer networks it is a barrier between some (more secure) internal network and a (less secure) outside network (i.e. the Internet)
- A firewall filters traffic
- Security rules define what can get through and what is blocked (in both directions in and out)

Packet filter firewall

- Operates on Network layer (and above)
- Filters based on source and destination IP Addresses, protocols, ports, current stage of a connection
- Static filtering rule set
- Standard security mechanisms and cost-effective

How does it work?

- Firewall software inspects the first few bytes of TCP or UDP headers in an IP packet
- Finds application protocol and port (e.g. HTTP with port 80 or SMTP with port 25)

How does it work?

- Often, traffic from inside out is allowed (except when explicitly blocked)
- One would for example block network management traffic (SNMP on UDP ports 161, 162)
- Traffic from outside in should be blocked if not explicitly permitted

Which traffic should be permitted?

- Different rules for existing connections and new connections
- Depends on applications/services running behind the firewall

Minimum information one needs to define:

- Source IP address (or range)
- Destination IP address (or range)
- Destination port (or range)

Source IP addresses examples:

- Any address should be able to connect to a web server.
- Management access should be restricted to specific IP addresses.

Destination IP addresses examples:

- IP address of the server running a service that should be accessed.
- Destination address needs to be defined.
- Never allow any IP address

Destination port examples:

- Specifies the service accessed via a particular port.
- Example: A Web-server needs incoming connections on port 80 (HTTP) and port 443 (HTTPS).
- Never allow any port

Where to place a firewall

- Firewall software on PCs is essential, but not sufficient
- In a home network, the router usually also acts as a firewall
- Proper placing in a company network is important

Even a very simple company network has:

- an internal network with PCs, servers, printers, etc.
- mail server, web-server, VPN gateway, etc.

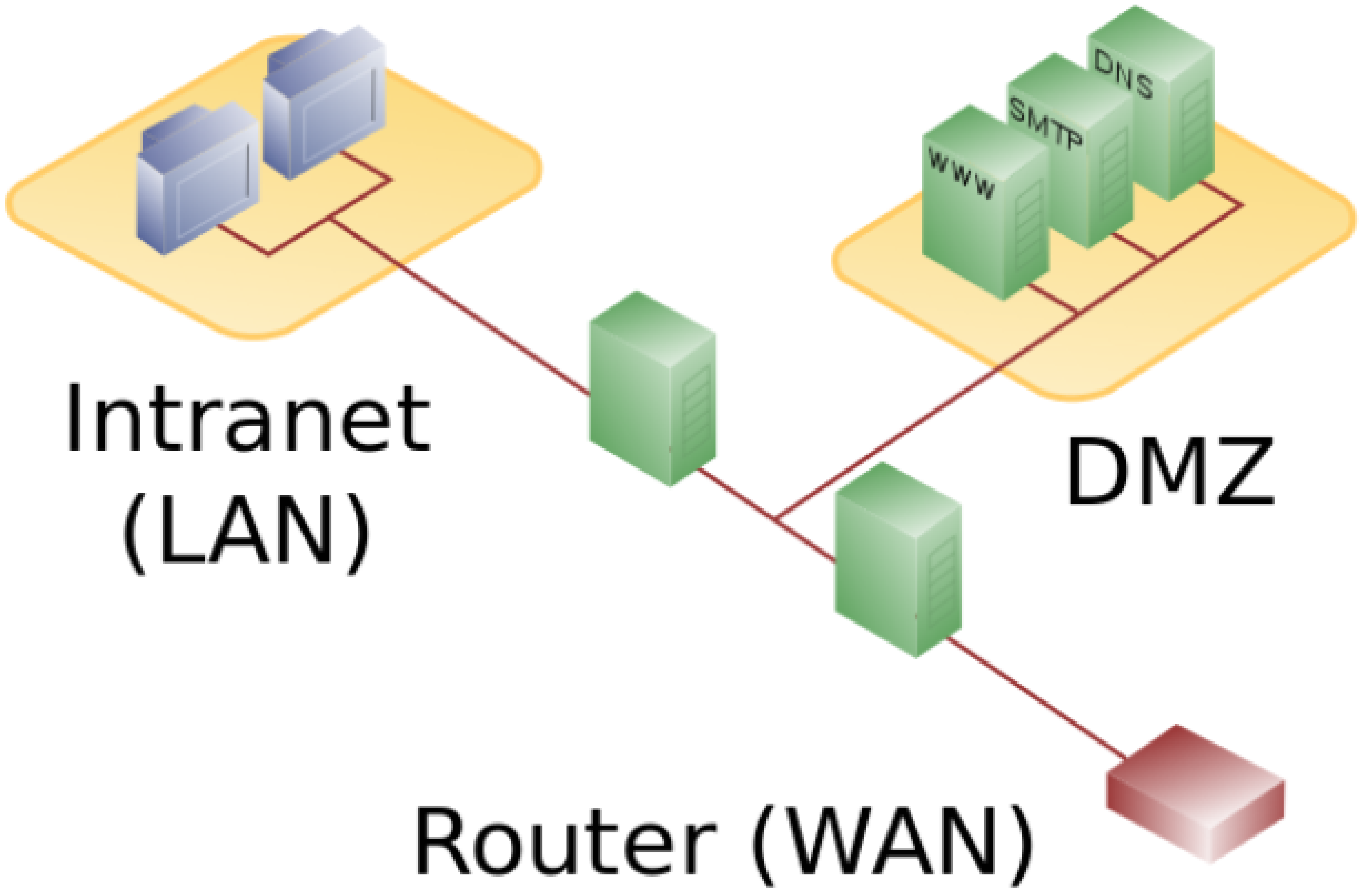
The internal network should not be directly accessible.

Web server or mail server need to be accessible.

DMZ - demilitarized zone

Create a zone that is considered to be less secure than the internal network, but still protected from direct access.

DMZ with two firewalls



(Wikimedia Commons)

Filtering outgoing traffic

Some examples:

- Prevent malicious software to send out data
- Block IP spoofing
- Block outbound traffic from critical network areas or computers
- Only allow outbound HTTP traffic through a proxy
- Logging of denied outbound traffic can help to detect infections

Proxies and NAT

Firewalls also provide

- Network and port-address translation (NAT). Internal network uses internal IP addresses not visible to the outside
- Proxies (e.g. for HTTP) can hide individual devices in the internal network

Not directly security functionalities, but hide some information from outside attackers.

Why firewalls are not enough

More and more applications connect internal networks to the Internet:

- Social networks
- Remote access (TeamViewer, RDP, etc.)
- Unified messaging (Skype, WeChat, etc.)
- Collaboration tools (Google Docs, OneNote, OneDrive, iCloud, etc.)

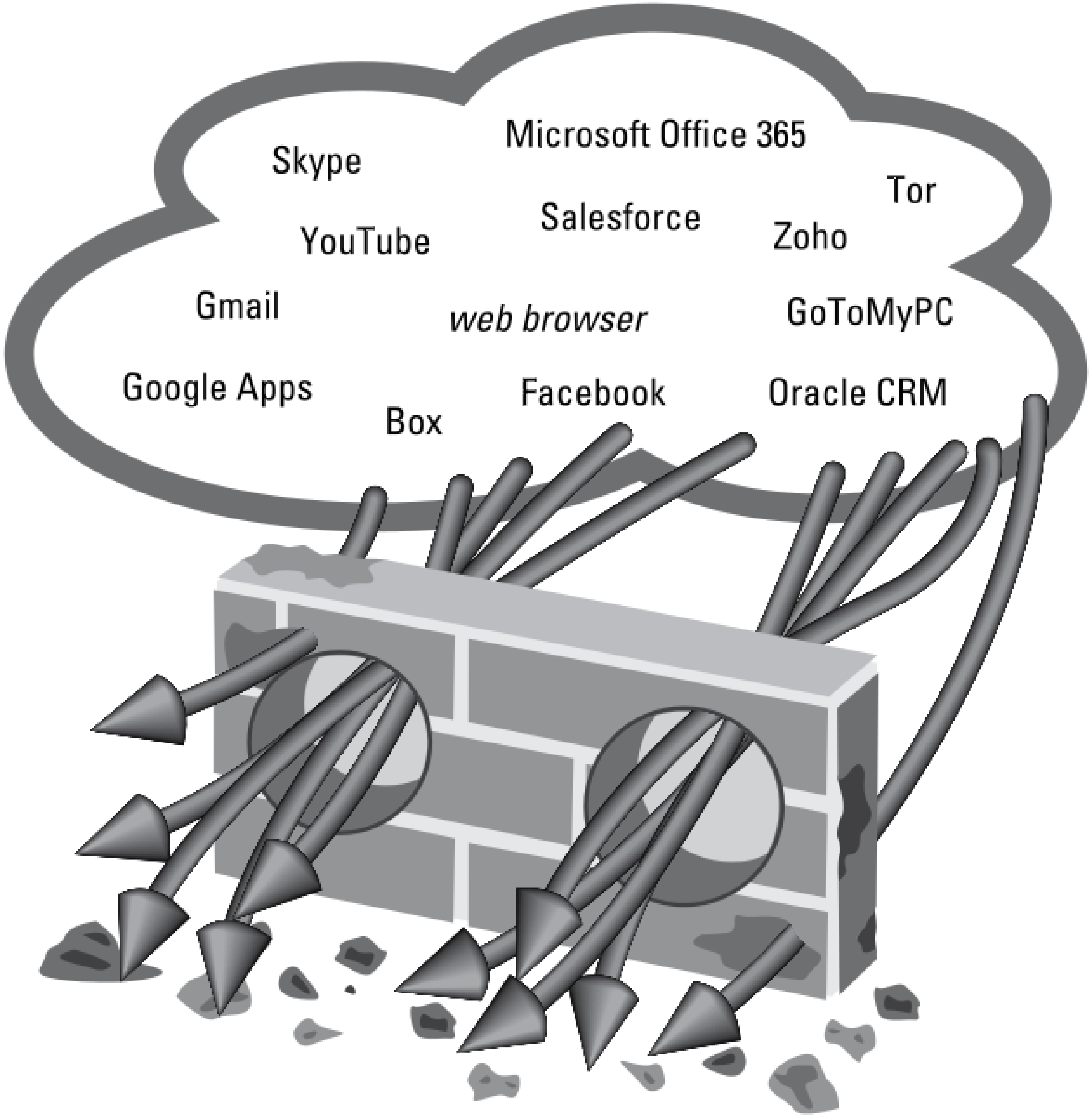
More difficulties

- Port hopping: Applications change their ports during a session
- Hiding in TLS encryption: TLS can mask application traffic (e.g. via TCP port 443)
- Appilcations use non-standard ports
- Tunnel in other services: Example is peer-to-peer file-sharing or messengers running over HTTP

Perimeter security has obvious constraints

- Firewalls don't help against internal attackers
- Once an attack was successful, firewalls cannot help
- Internet of things, mobile networks, etc.

Cannot control applications



(NGF for Dummies; John Wiley and Sons)

IDS and IPS

IDS - Intrusion Detection System

- Monitors network and/or system activities.
- Alert when potentially malicious activity is found.
- Logs information about activities.

IDS and IPS

IPS - Intrusion Prevention System

- IDS with additional active functionality.
- Attempts to block or stop malicious activities.

Monitoring actions (examples)

- Detect port scans
- Detect OS fingerprinting attempts
- Look for specific attacks (e.g. buffer overflow)
- Find and block known malware
- Detect server massage block (SMB) probes
- Find anomalies

Reactions (examples)

- Drop malicious packets and send alarm
- Block traffic from some IP addresses
- Correct fragmentation in packet streams

Raise alerts

Might trigger human intervention by incident response teams.

IDS/IPS should use anomaly-based detection as well as signature-based detection.

- Signature-based is fast, generates less false positives and does not need a learning phase.
- Anomaly-based can detect unknown attacks

Next-generation firewalls (NGF)

- Promise an integrated security approach
- Proxy for all traffic (even encrypted)
- Might become very powerful security tools
- Look at applications, logical segments, roles, services, users, etc.

Potential NGF problems

- Policy rules get too complex
- Proxy for TLS etc. breaks end-to-end security
- Encapsulated encryption still possible
- Privacy issues
- Single point of attack with full access to decrypted data

The Security Impact of HTTPS Interception

Zakir Durumeric at. al. NDSS'17,

26 February–1 March, 2017, San Diego, CA, USA http://dx.doi.org/10.14722/ndss.2017.23456

HTTPS Interception

News from August 2016:

- Cisco Systems has confirmed that recently-leaked malware tied to the National Security Agency exploited a high-severity vulnerability that had gone undetected for years in every supported version of the company's Adaptive Security Appliance (ASA) firewall.
- People within the US government have known of the risk since at least 2013 and allowed it to persist.

Why is this CISCO vulnerability a problem?

- The ASA also stores VPN keys that can be compromised.
- An attacker can change the firewall configuration.
- An attacker could create backdoors to many networks.
- Logging of malicious traffic can be prevented.

Virus Scanner - Anti-Virus Software

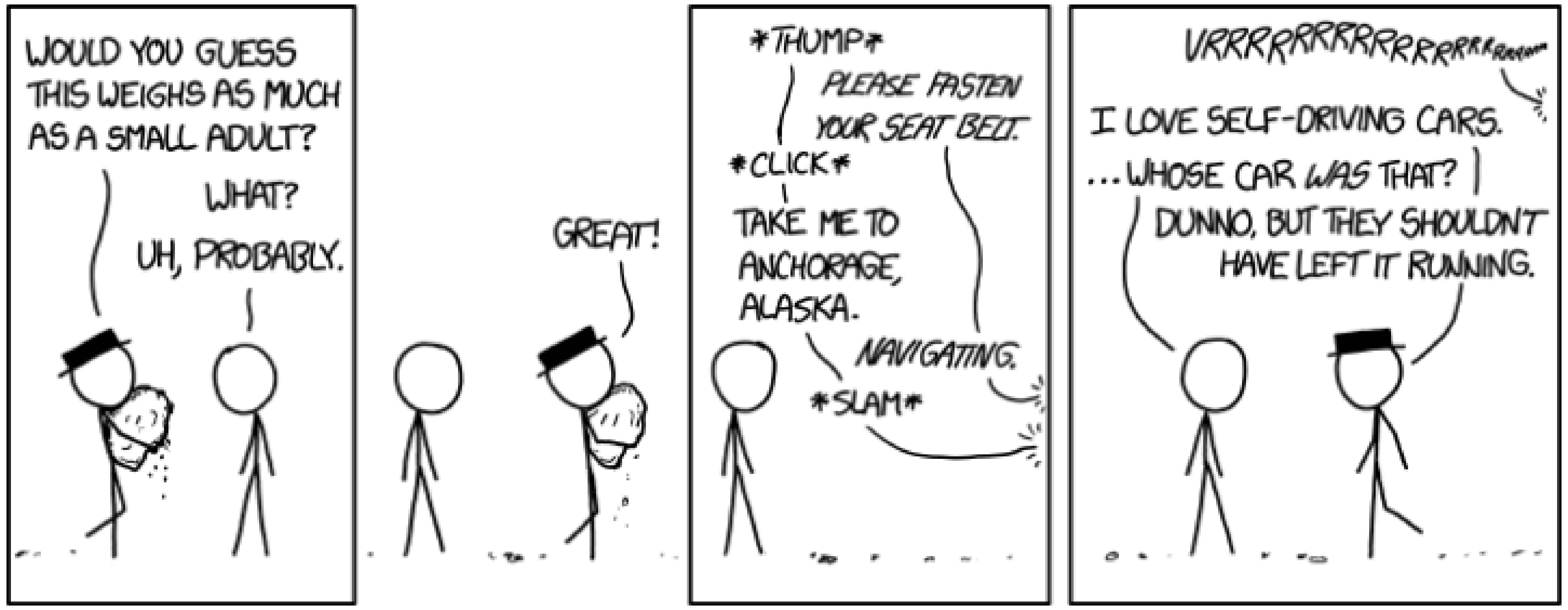
Virus Scanner - Anti-Virus Software

- Anti-Virus Software can efficiently prevent infections with known malware.
- Is the first thing to be manipulated by malware.
- Unable to detect new malware.

Additionl vulnerabilities through Anti-Virus Software

https://bugs.chromium.org/p/project-zero/issues/detail?id=693&redir=1

There are many ways to attack systems


WOULD YOU GUESS THIS WEIGHS AS MUCH AS A SMALL ADULT?
WHAT?
UH, PROBABLY.
GREAT!
THUMP
PLEASE FASTEN YOUR SEAT BELT.
CLICK
TAKE ME TO ANCHORAGE, ALASKA.
NAVIGATING.
SLAM
VRRRRRRRRRRRRRRRRR
I LOVE SELF-DRIVING CARS.
...WHOSE CAR WAS THAT?
DUNNO, BUT THEY SHOULDN'T HAVE LEFT IT RUNNING.

(xkcd.org)

Nicely shows that not all security issues are technical...