FIT 1047

Introduction to computer systems, networks and security

MONASH University

Overview for today

- 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

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?

- 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)
- Often, traffic from inside out is allowed (except when explicitly blocked)

How does it work?

- Often, traffic from inside out is allowed (except when explicitly blocked)
- One would for example block network management traffic from inside out (SNMP on UDP ports 161, 162)

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

Which traffic should be permitted?

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

On needs to define:

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

Source IP addresses:

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

Destination IP addresses:

- 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:

- Specifies the service accessed via a particular port.
- Example: A Webserver needs incoming connections on port 80 (http) and port 443 (https).
- Nerver allow any port

Where to place a firewall

- Firewall software on PCs is essential, but not sufficient

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

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, webserver, VPN gateway, etc.

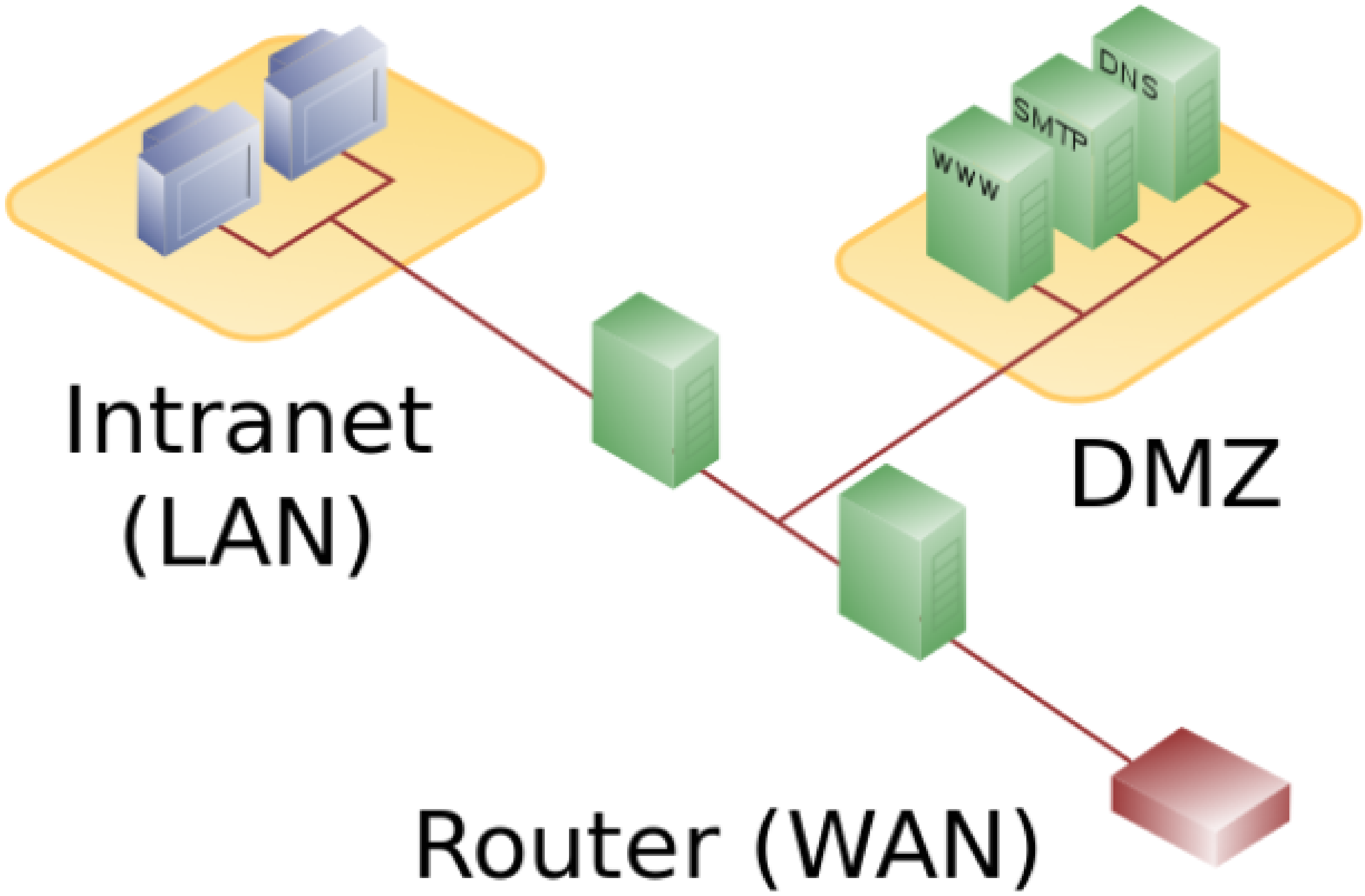
The internal network should not be directly accessible.

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 proxie
- 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.)

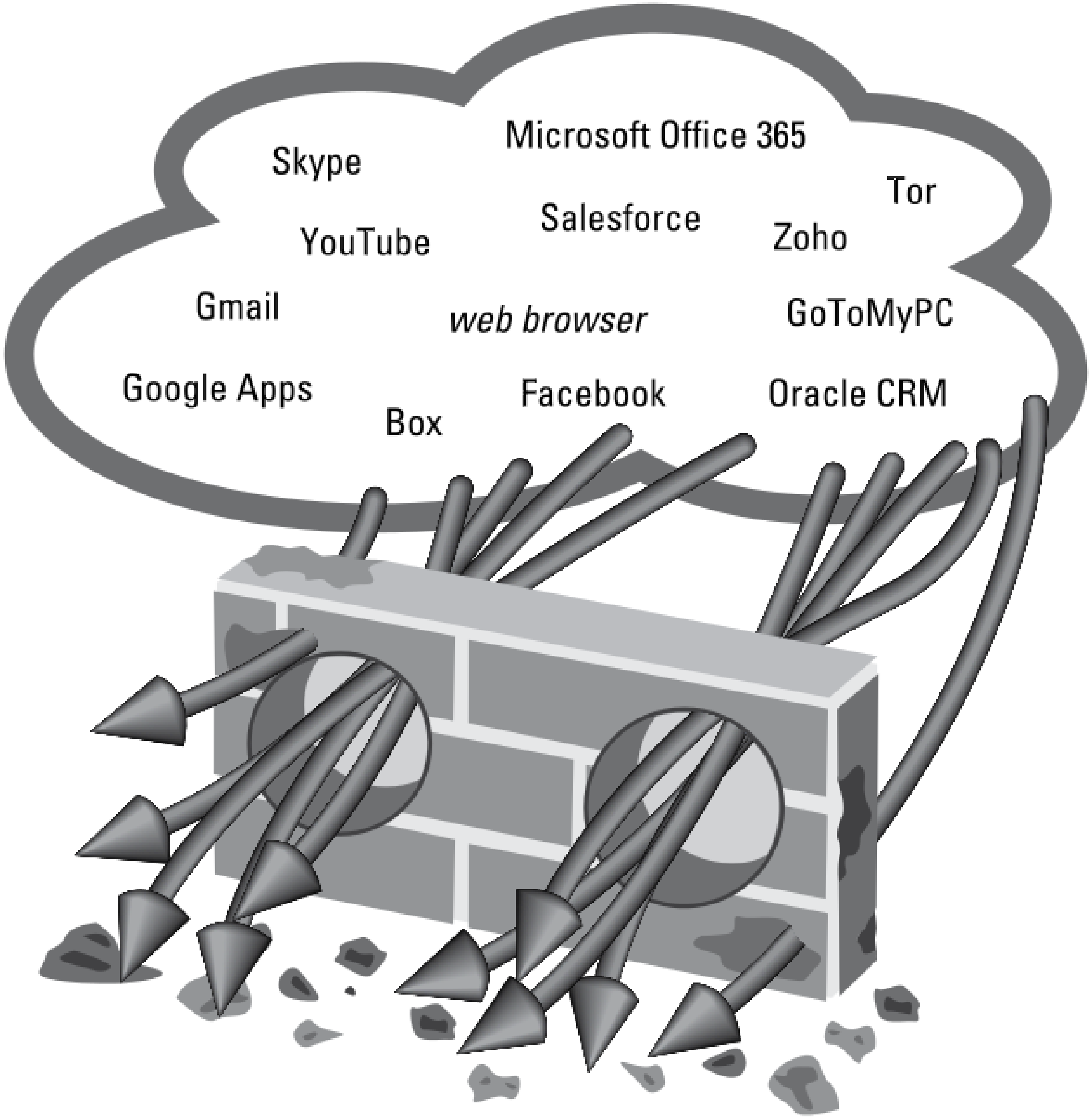
More difficulties

- Port hopping: Applications change their ports during a session
- Hiding in TLS encryption: TLS can mask application traffic (e.g. via TCP port 443)
- Don't use 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

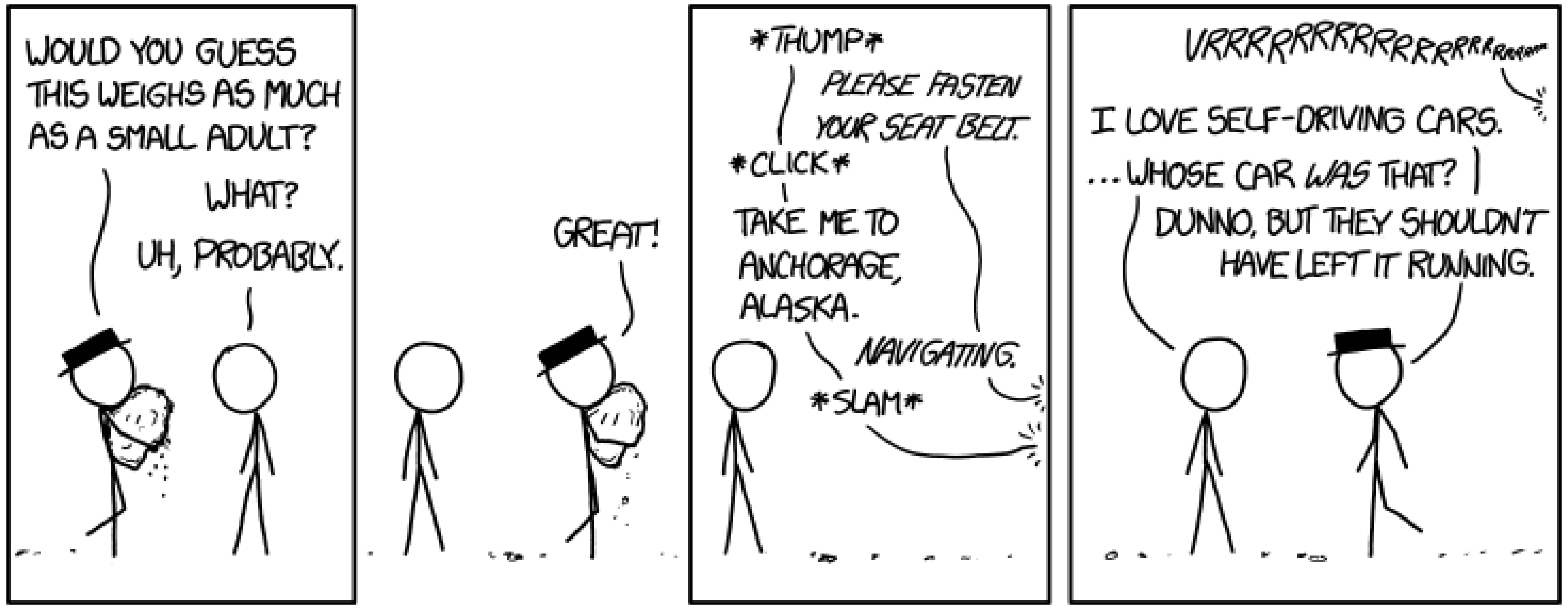
Next-generation firewalls (NGF)

- 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

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
VRRRRRRRRRRRRRRRrrrrm
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...

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.