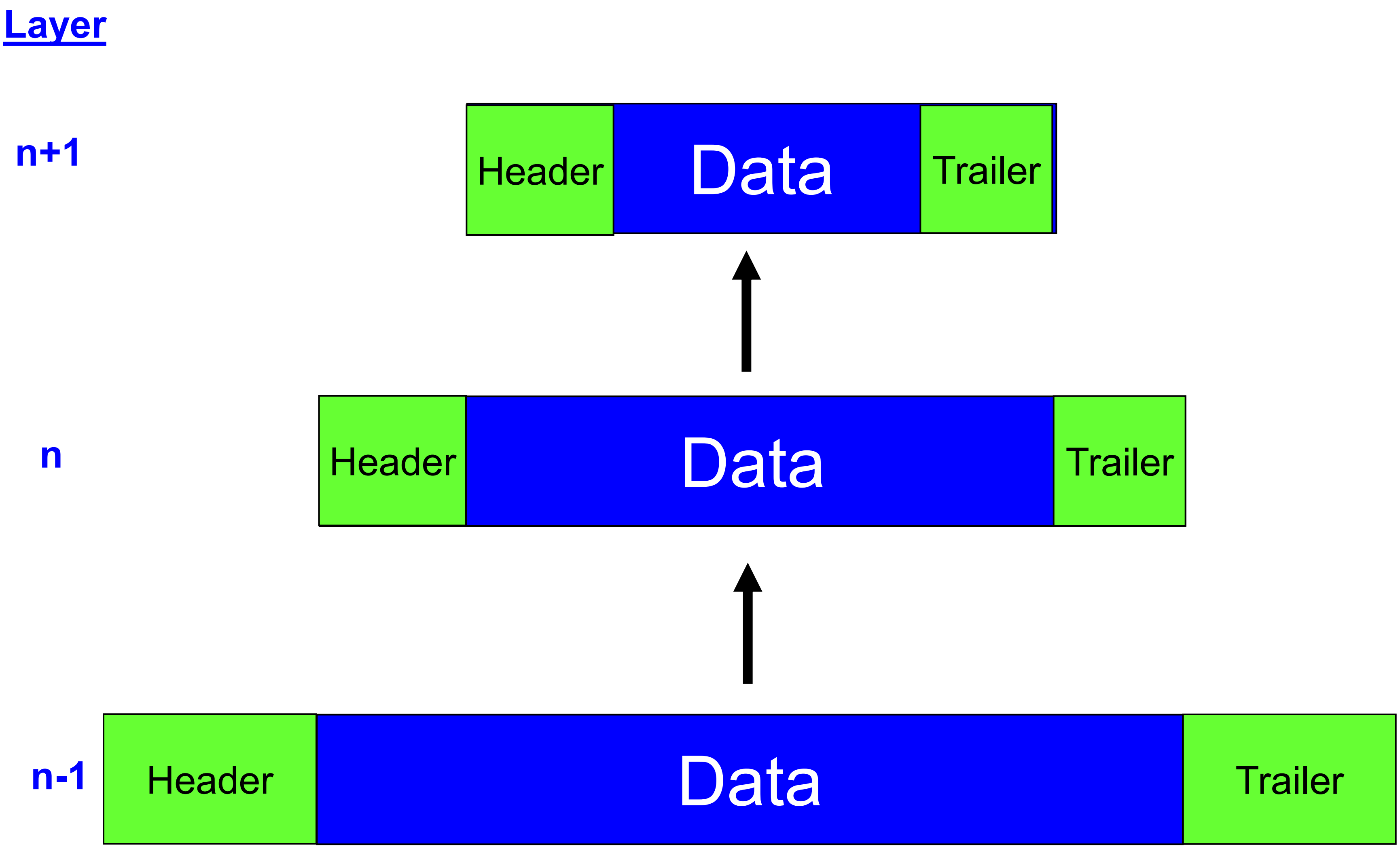
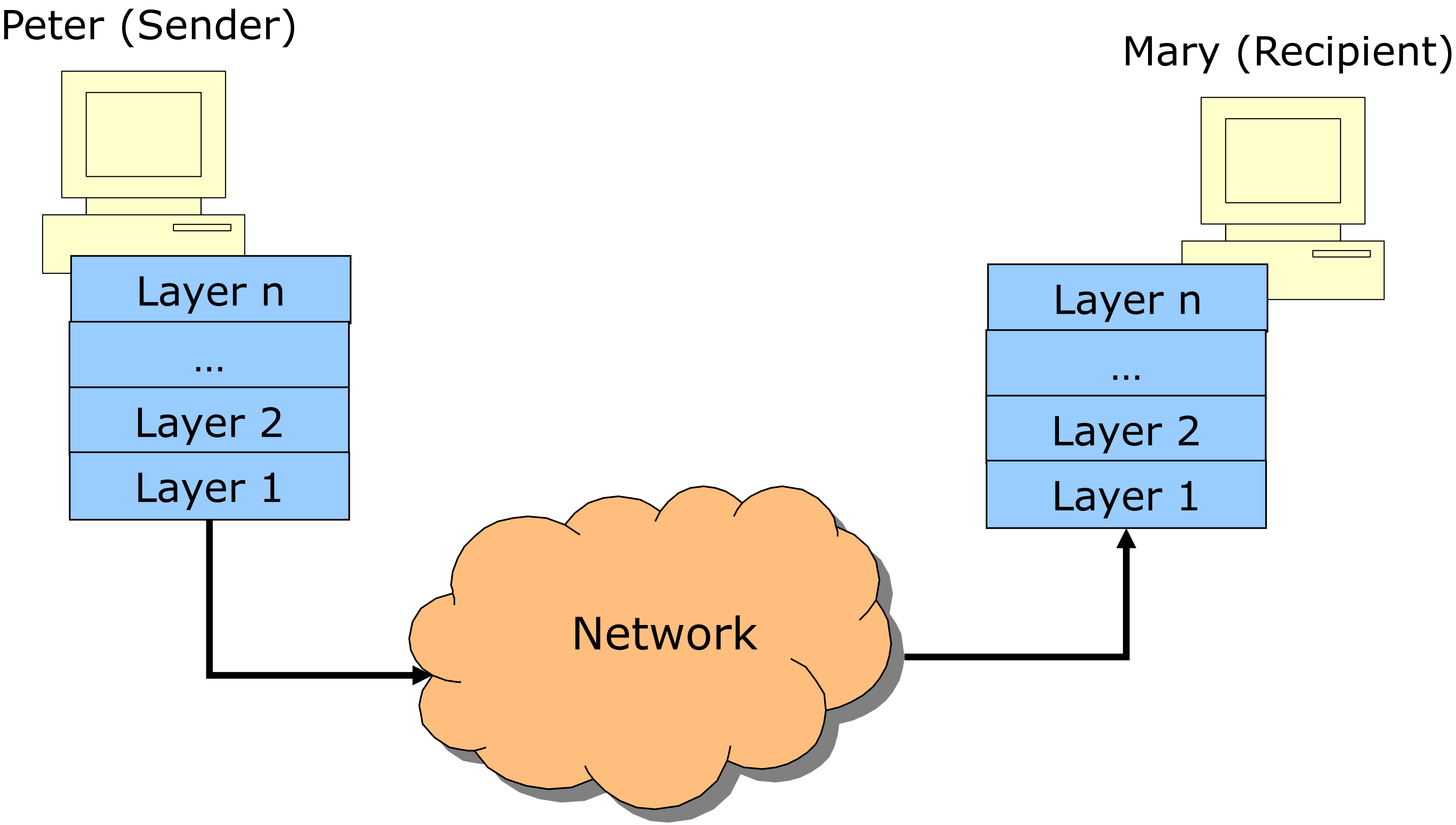
Layer Data

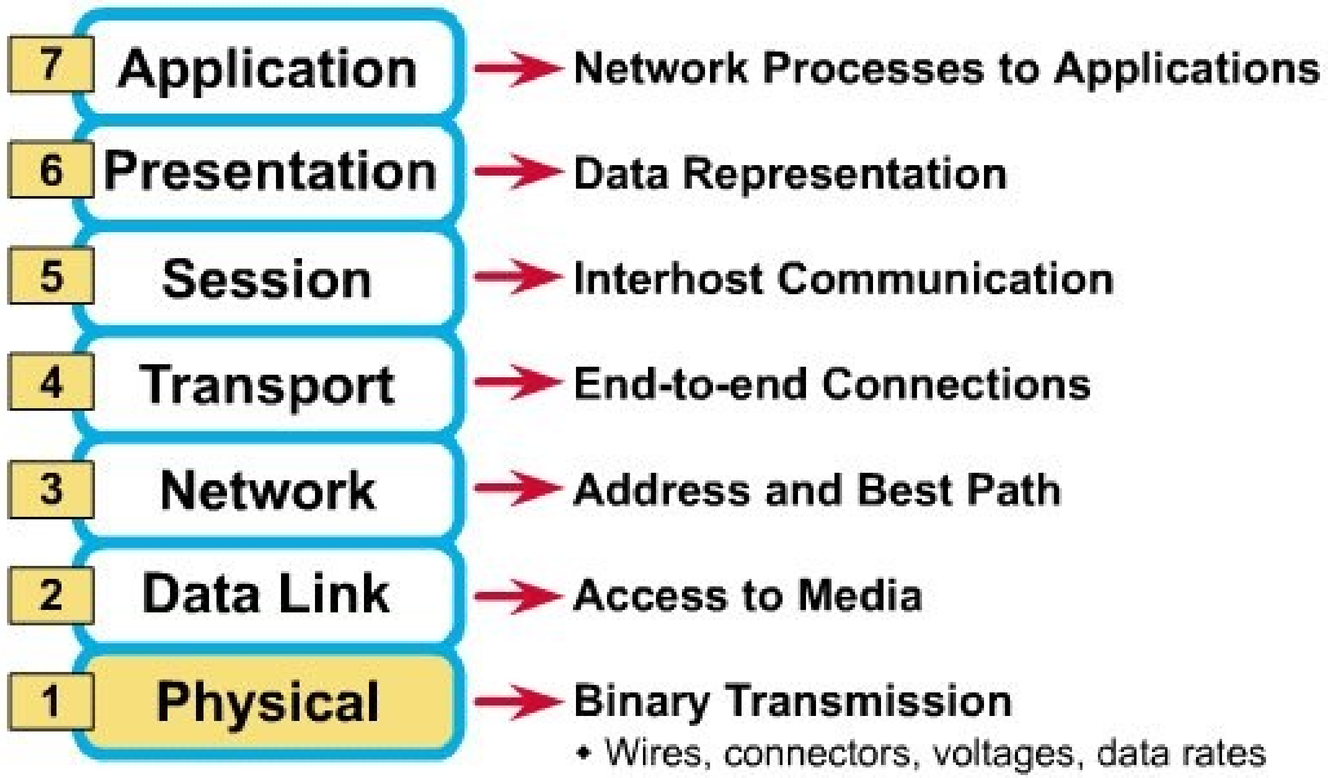

Layer
n+1
Header
Data
Trailer
n
Header
Data
Trailer
n-1
Header
Data
Trailer

Layer-based Inter-Computer Communication



OSI Reference Model

- The OSI Reference Model is a “reference guide” for understanding network functionality.
- Each of the 7 layers (numbered from bottom to top) represents one step in the process of sending data packets from a source to a destination.



7 Application → Network Processes to Applications

6 Presentation → Data Representation

5 Session → Interhost Communication

4 Transport → End-to-end Connections

3 Network → Address and Best Path

2 Data Link → Access to Media

1 Physical → Binary Transmission

- Wires, connectors, voltages, data rates

The Postal Analogy

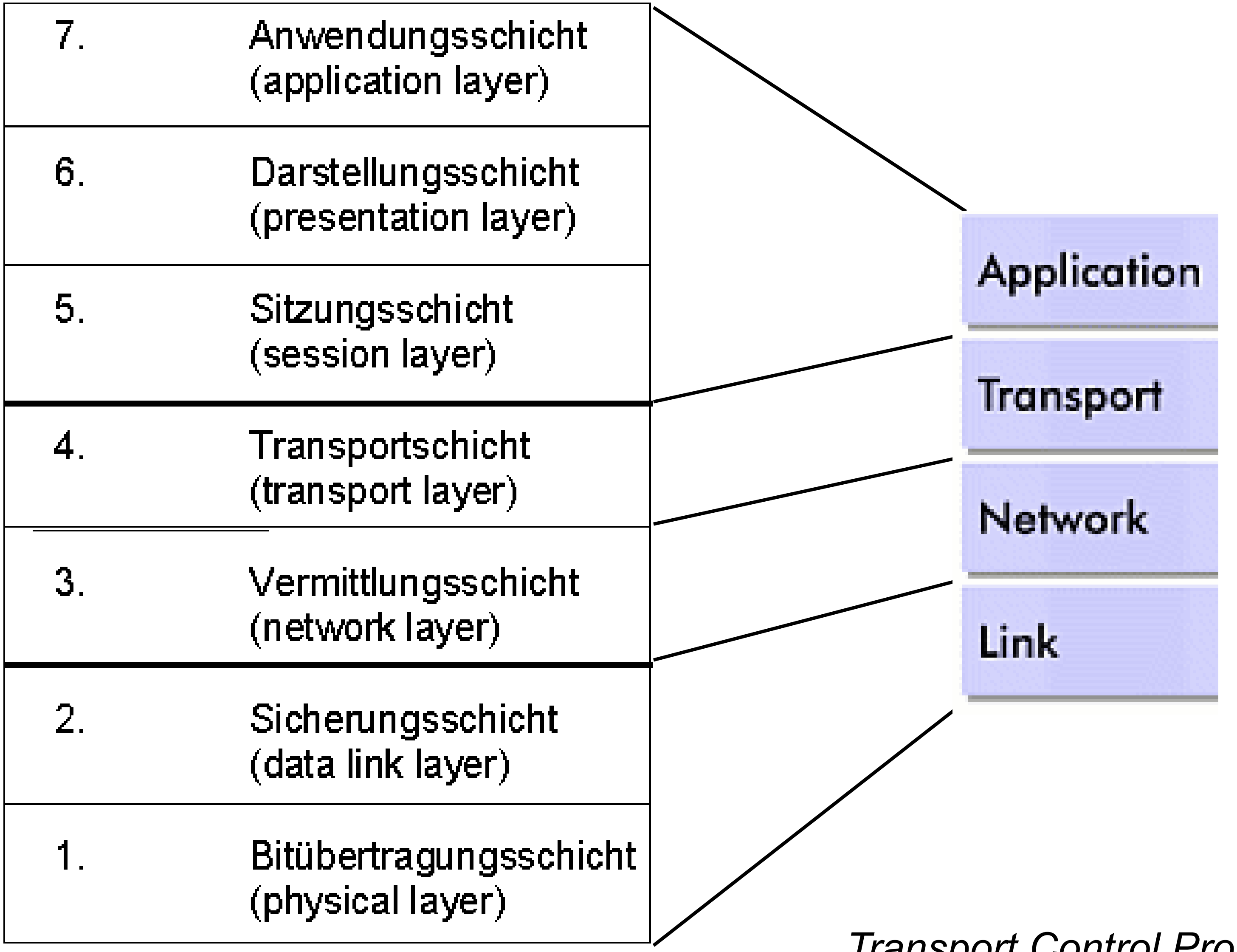
How would the OSI compare to the regular Post Office

- Application
- Presentation
- Session
- Transport
- Network
- Data-Link
- Physical

- **A-** Write a 20 page letter to a foreign country.
- **P-** Translate the letter so the receiver can read it.
- **S-** Insure the intended recipient can receive letter.
- **T-** Separate and number pages. Like registered mail, tracks delivery and requests another package if one is “lost” or “damaged” in the mail.
- **N-** Postal Center sorting letters by zip code to route them closer to destination.
- **D-** Local Post Office determining which vehicles to deliver letters.
- **P-** Physical Trucks, Planes, Rail, autos, etc which carry letter between stations.

"All People Seem To Need Data Processing"

OSI Reference Model and TCP/IP Protocol



7.	Anwendungsschicht (application layer)
6.	Darstellungsschicht (presentation layer)
5.	Sitzungsschicht (session layer)
4.	Transportschicht (transport layer)
3.	Vermittlungsschicht (network layer)
2.	Sicherungsschicht (data link layer)
1.	Bitübertragungsschicht (physical layer)

- Application
- Transport
- Network
- Link

OSI Model

Transport Control Protocol/ Internet Protoocol

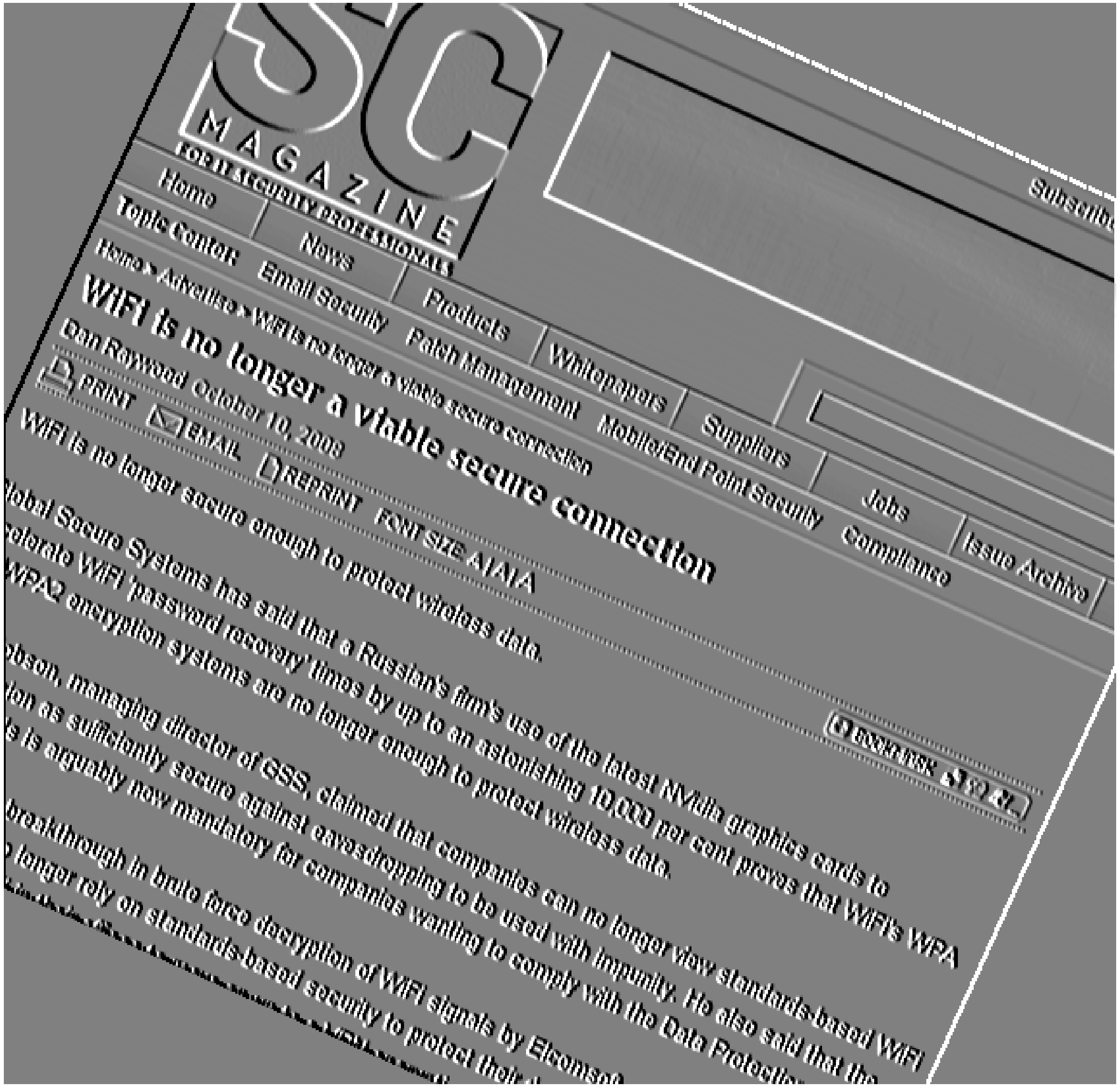
Internet Protocol Suite

- 5. Application Layer
  - DHCP · DNS · FTP · Gopher · HTTP · IMAP4 · IRC · NNTP · POP3 · SIP · SMTP · SNMP · SSH · TELNET · RPC · SOAP · NTP · …
- 4. Transport Layer
  - TCP · UDP · …
- 3. Network/Internet Layer
  - IP (IPv4 · IPv6) · IPsec · ARP · RARP · …
- 2. Data Link Layer
  - 802.11 (WLAN) · (Wi-Fi) · WiMAX · ATM · Token ring · Ethernet · FDDI · GPRS · PPP · ISDN · …
- 1. Physical Layer
  - Ethernet physical layer · Modems · Optical fiber · Coaxial cable · Twisted pair · …

Source: en.wikipedia.org

WiFi is secure, but...

Is Wifi still secure?



WiFi is no longer a viable secure connection

Dan Raywood October 10, 2008

WiFi is no longer secure enough to protect wireless data.

lobal Secure Systems has said that a Russian's firm's use of the latest NVidia graphics cards to
celerate WiFi 'password recovery' times by up to an astonishing 10,000 per cent proves that WiFi's WPA
WPA2 encryption systems are no longer enough to protect wireless data.

obson, managing director of GSS, claimed that companies can no longer view standards-based WiFi
ion as sufficiently secure against eavesdropping to be used with impunity. He also said that the
s is arguably now mandatory for companies wanting to comply with the Data Protection

breakthrough in brute force decryption of WiFi signals by Elcomsoft
longer rely on standards-based security to protect their

WiFi is no longer a viable secure connection?

tinyurl.com/4sq5fn

- Wifi (WPA, WPA2) is said to be "secure"
- Max. Password Length: 63

Characters	
A-Z	26
a-z	26
0-9	10
äüö/\?!-&%$"()=+#ß	18
Sum:	80

- Can only be attacked by "brute-force" attacks
- Russian Company ELMSOFT announces in 2008 "to break Wi-Fi encryption up to 100 times faster than by using CPU only" (tinyurl.com/4585wv)
- Should be all return to cable-based networks?

The Approach of Wifi Hacking

- Logging of Network Traffic (esp. Authentication)
- Offline Brute-Force Attack (pot. dictionary-based)

- Max. Password Length: 63, Number of Characters: 80
  - -> 80^n permutations for a password of length n

- Dictionaries can speed-up the hacking... however
  - language-specific dictionaries are required ("Vogel", "Bird", "Uccello")
  - what about combination of words and numbers/spec. characters like
    - "Vogel0815", "Bird;!$%&", ...

How long does it actually take?

Passwort Length	Permutations	100 PWs/sec (years)	1000 PWs/sec (years)	100.000 PWs/sec (years)	1 Mio. PWs/sec (years)	10 Mio. PWs/sec (years)	100 Mio. PWs/sec (years)
1	80	2,53678E-08	2,53678E-09	2,53678E-11	2,53678E-12	2,53678E-13	2,53678E-14
2	6400	2,02943E-06	2,02943E-07	2,02943E-09	2,02943E-10	2,02943E-11	2,02943E-12
3	512000	0,000162354	1,62354E-05	1,62354E-07	1,62354E-08	1,62354E-09	1,62354E-10
4	40960000	0,012988331	0,001298833	1,29883E-05	1,29883E-06	1,29883E-07	1,29883E-08
5	3276800000	**1,039066464**	0,103906646	0,001039066	0,000103907	1,03907E-05	1,03907E-06
6	2,62144E+11	83,1253171	**8,31253171**	0,083125317	0,008312532	0,000831253	8,31253E-05
7	2,09715E+13	6650,025368	665,0025368	**6,650025368**	0,665002537	0,066500254	0,006650025
8	1,67772E+15	532002,0294	53200,20294	532,0020294	**53,20020294**	**5,320020294**	0,532002029
9	1,34218E+17	42560162,35	4256016,235	42560,16235	4256,016235	425,6016235	**42,56016235**
10	1,07374E+19	3404812988	340481298,8	3404812,988	340481,2988	34048,12988	3404,812988
20	1,15292E+38	3,65589E+28	3,65589E+27	3,65589E+25	3,65589E+24	3,65589E+23	3,65589E+22
30	1,23794E+57	3,92548E+47	3,92548E+46	3,92548E+44	3,92548E+43	3,92548E+42	3,92548E+41
40	1,32923E+76	4,21495E+66	4,21495E+65	4,21495E+63	4,21495E+62	4,21495E+61	4,21495E+60
50	1,42725E+95	4,52577E+85	4,52577E+84	4,52577E+82	4,52577E+81	4,52577E+80	4,52577E+79
60	1,5325E+114	4,8595E+104	4,8595E+103	4,8595E+101	4,8595E+100	4,8595E+99	4,85951E+98
63	7,8464E+119	2,4881E+110	2,4881E+109	2,4881E+107	2,4881E+106	2,4881E+105	2,4881E+104

Core2 Duo: ~1.000 PWs/sec.
-> 100 times faster: 100.000 PWs/sec.
-> 100 PCs: 10 Mio. PWs/sec

Exercise 1.2