Základy bezpečnosti TCP/IP sietí

Ing. Radovan Semančík

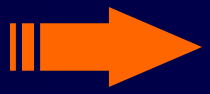
Základy bezpečnosti TCP/IP

- Úvod
- Základy TCP/IP
- Problémy bezpečnosti TCP/IP
- Filtrovanie TCP/IP - Firewall
- Záver

Úvod

- TCP/IP - Transmission Control Protocol/Internet Protocol
  - Základ Internetu (ARPANET)
  - Prepájanie lokálnych sietí
  - ARPANET z počiatku uzavretý => nízka potreba zabezpečenia
  - Súčasnosť: Internet = komerčné médium
  - Potreba zabezpečovania služieb

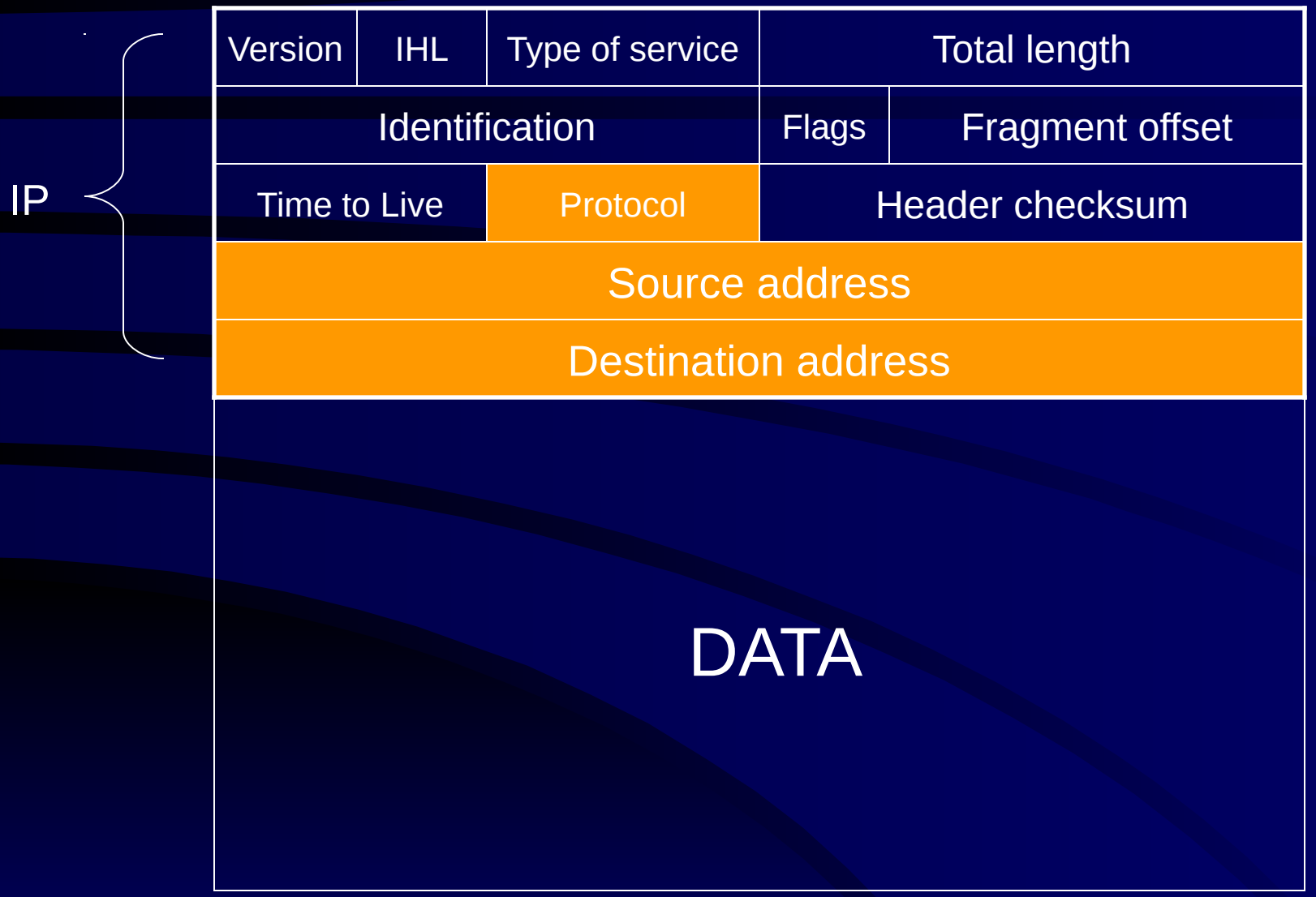
Základy bezpečnosti TCP/IP



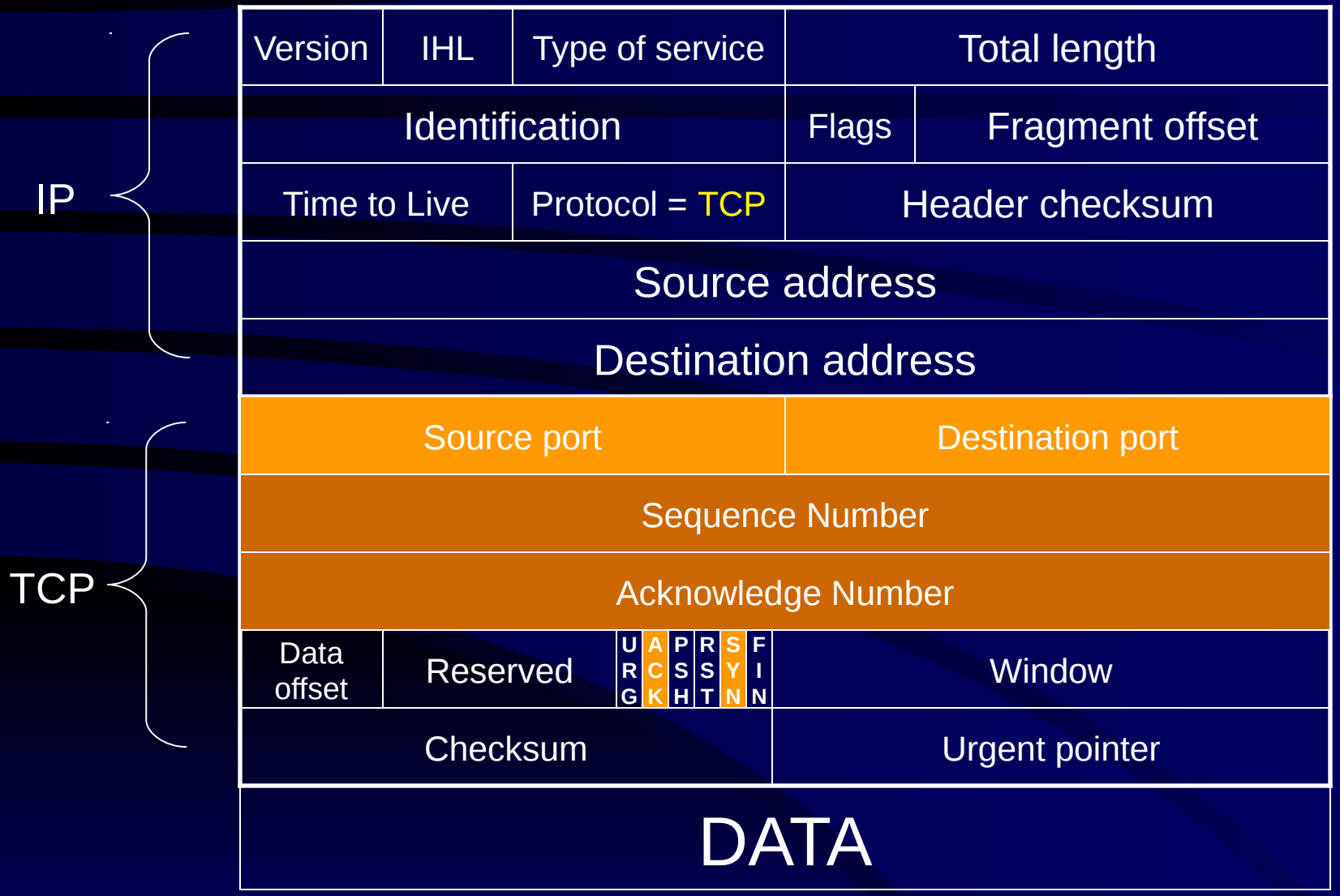
- Úvod
- Základy TCP/IP
  - Referenčný model
  - TCP/IP hlavičky
  - TCP Spojenie
- Problémy bezpečnosti TCP/IP
- Filtrovanie TCP/IP - Firewall
- Záver

Referenčný model

TCP/IP Hlavičky

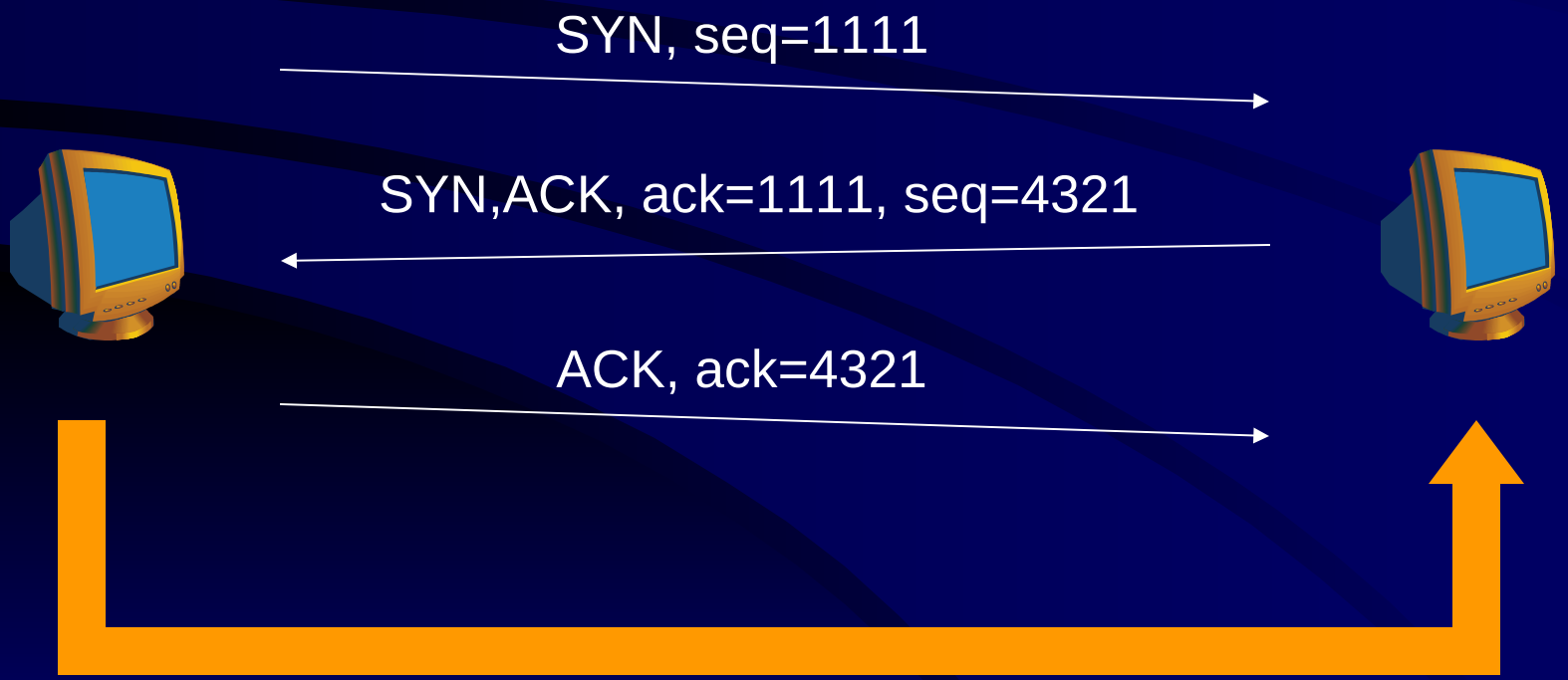


TCP/IP Hlavičky



TCP spojenie

Otvorenie spojenia
(three-way handshake)



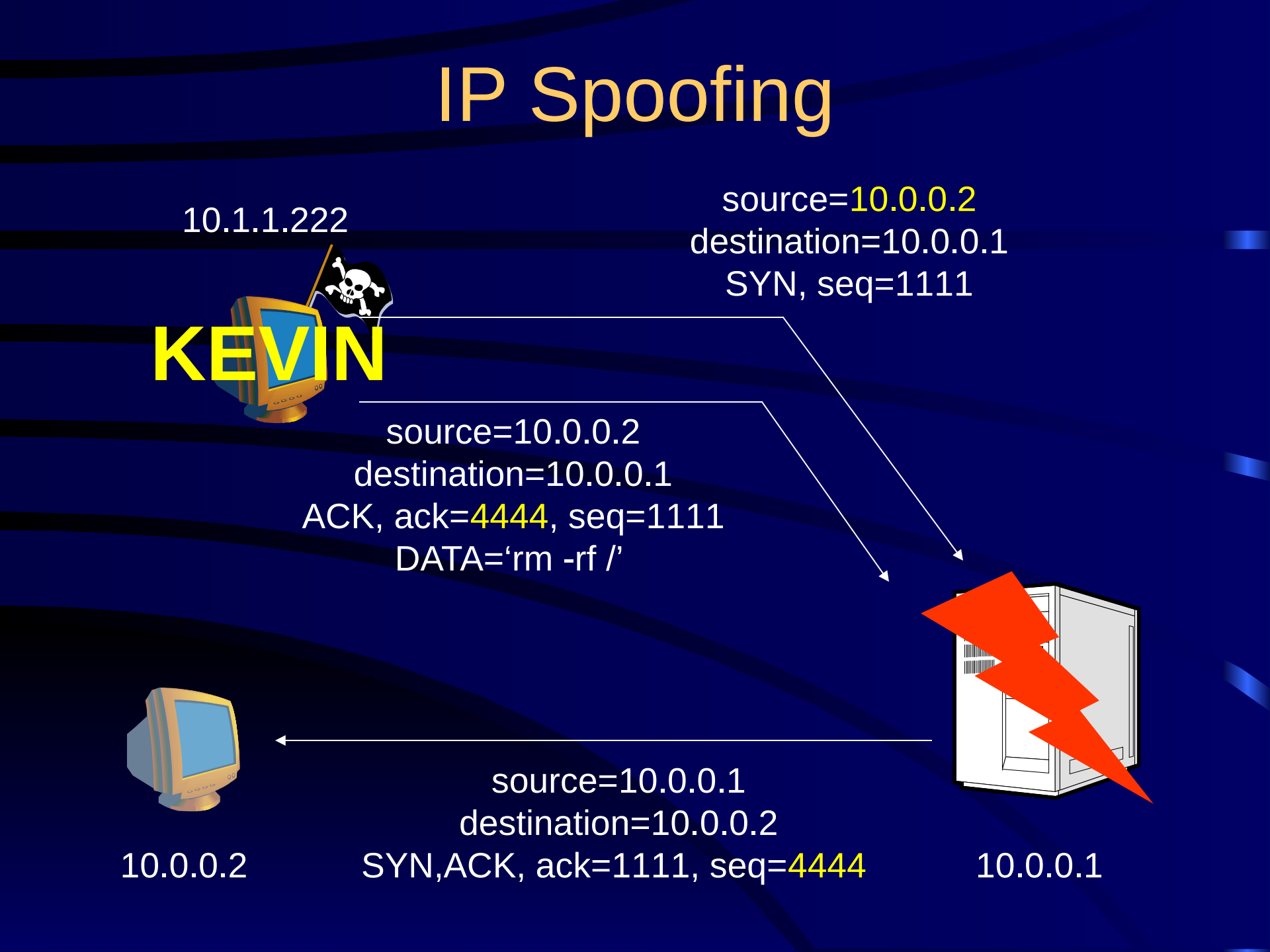
TCP spojenie

Prenos údajov

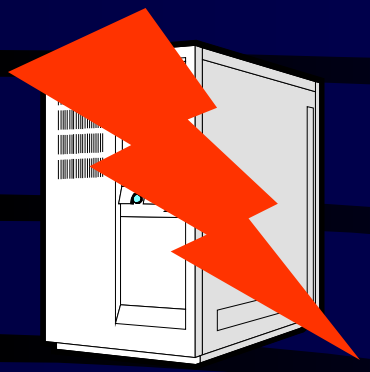
Základy bezpečnosti TCP/IP

- Úvod
- Základy TCP/IP
- Problémy bezpečnosti TCP/IP
  - Spoofing a spol.
  - Bombardovanie - “flooding”
  - Aplikačné problémy
- Filtrovanie TCP/IP - Firewall
- Záver

IP Spoofing


10.1.1.222
KEVIN
source=10.0.0.2
destination=10.0.0.1
SYN, seq=1111
source=10.0.0.2
destination=10.0.0.1
ACK, ack=4444, seq=1111
DATA='rm -rf /'
source=10.0.0.1
destination=10.0.0.2
SYN,ACK, ack=1111, seq=4444
10.0.0.2
10.0.0.1

Hijacking

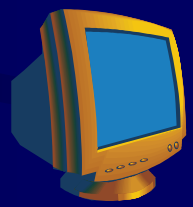


10.0.0.1

ACK, ack=4321, seq=1111, DATA='Password:'

ACK, ack=1120, seq=4327, DATA='medved'

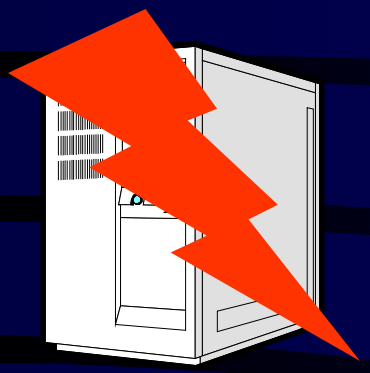
ACK, ack=4327, seq=1116



10.0.0.2

Source=10.0.0.2
destination=10.0.0.1
ACK, ack=1120, seq=4335, DATA='rm -rf /'

Flooding - bombardovanie

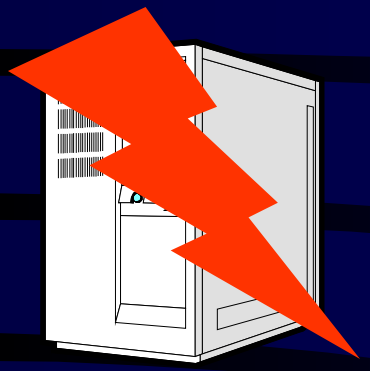


10.0.0.1

Source=10.1.1.222

10.1.1.222

SYN Flooding



10.0.0.1

Source=10.0.1.5, SYN, seq=5484

Source=10.3.8.14, SYN, seq=1287

Source=10.8.15.2, SYN, seq=5684

Source=10.8.15.2, SYN, seq=5684

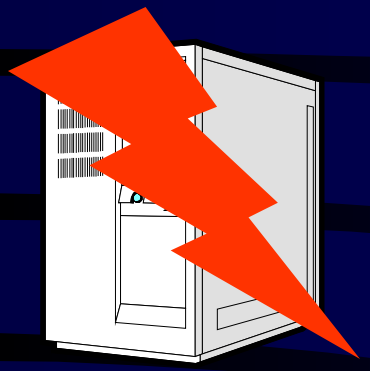
Source=10.1.54.89, SYN, seq=9547

Source=10.78.2.9, SYN, seq=7546

Source=10.5.88.45, SYN, seq=6045

10.1.1.222

Aplikačné problémy



10.0.0.1

finger papek@domena.sk

Real Name: Krepy Papek

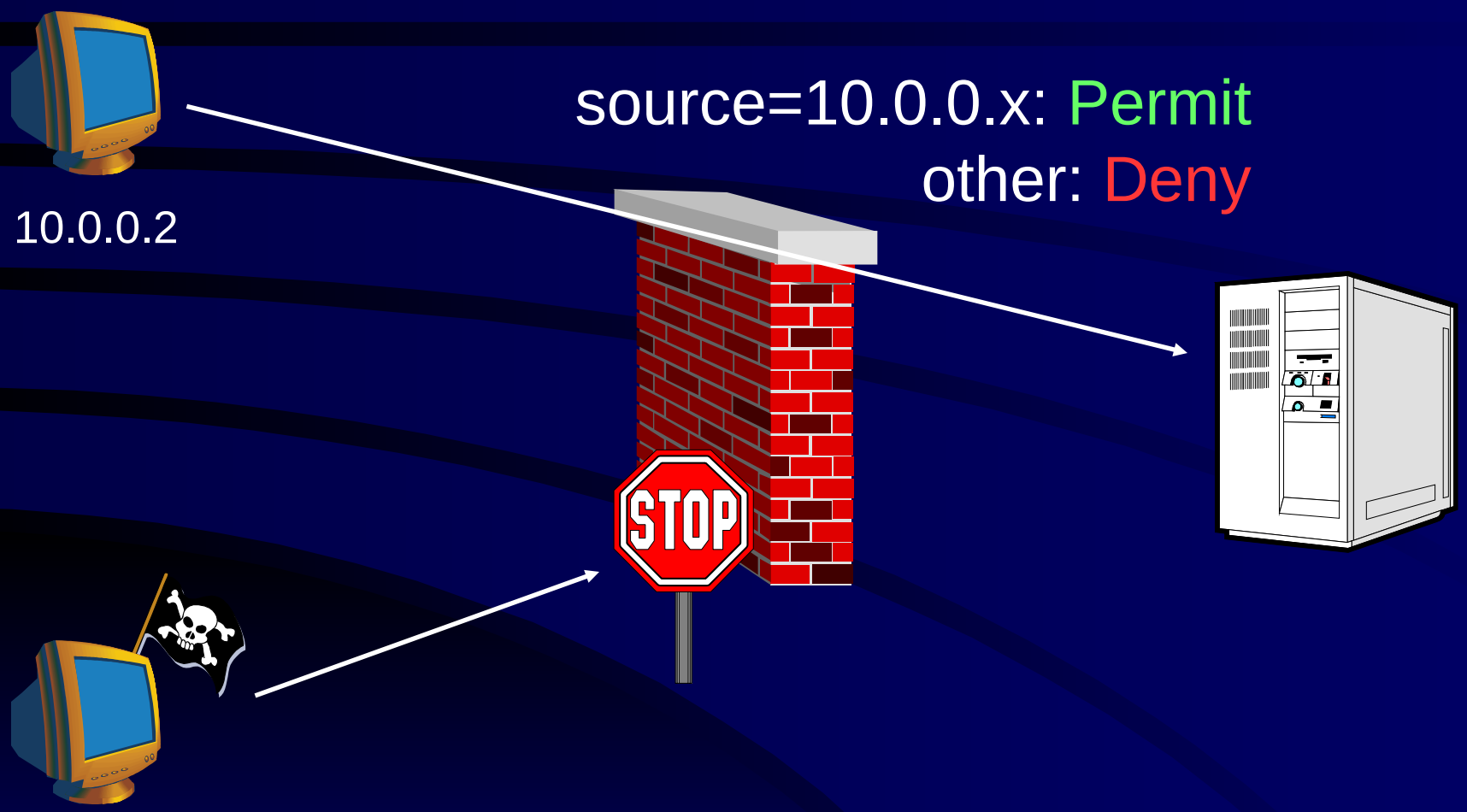
10.1.1.222

finger ÷¿Í®ø¿Tv÷¿½u÷¿¾Íù¿ûs÷¿%t÷¿
½Lö¿|Mö¿ö¿j@ö¿–+ö¿H+ö¿
Hö¿p,ö¿Lö¿Û"ö¿Kö¿Mö¿\
ö¿ûö¿ÍKö¿ÏQö¿Oö¿-ö¿‹Hö
¿Z+ö¿©#ö¿õ@ö¿Eö¿Mö¿1ö¿
¬&ö¿”-ö¿fö¿"Mö¿Rö¿_#ö¿¨M
ö¿PEö¿£Nö¿'Fö¿°ö¿Wö¿Kö
¿·#ö¿—Fö¿‘#ö¿Á#ö¿Ù8ö¿+Qö¿
+ö¿7#ö¿Zö¿¾ö¿}#ö¿öö¿y

Základy bezpečnosti TCP/IP

- Úvod
- Základy TCP/IP
- Problémy bezpečnosti TCP/IP
- Filtrovanie TCP/IP - Firewall
  - Druhy firewallov
  - Filtrovacie pravidlá
- Záver

Firewall

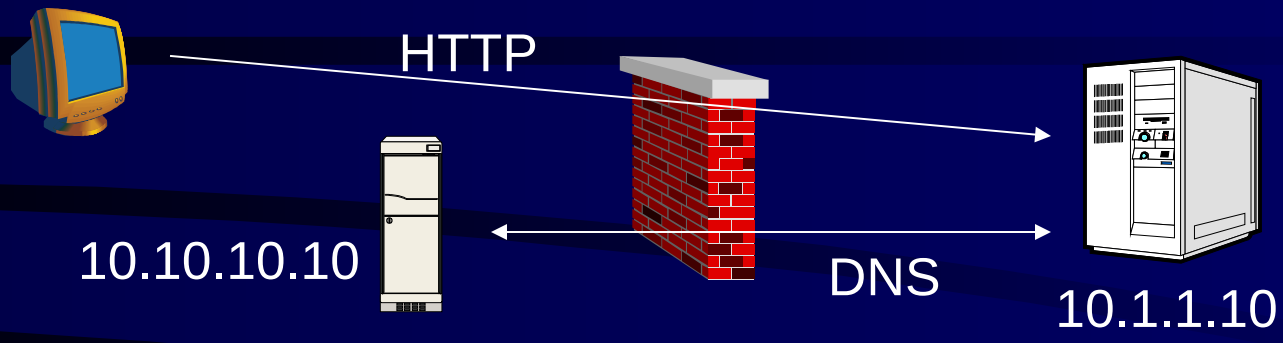


Druhy firewallov

- Bezstavový paketový filter
  - Málo bezpečný, lacný, veľmi bežný
  - Cisco ACL, Linux, …
- Stavový paketový filter
  - Bezpečný, vysoká cena, komplexný
  - CheckPoint FW-1, Cisco PIX
- Brána (Application gateway, proxy)
  - Veľmi bezpečná, minimálna flexibilita

Filtrovacie pravidlá

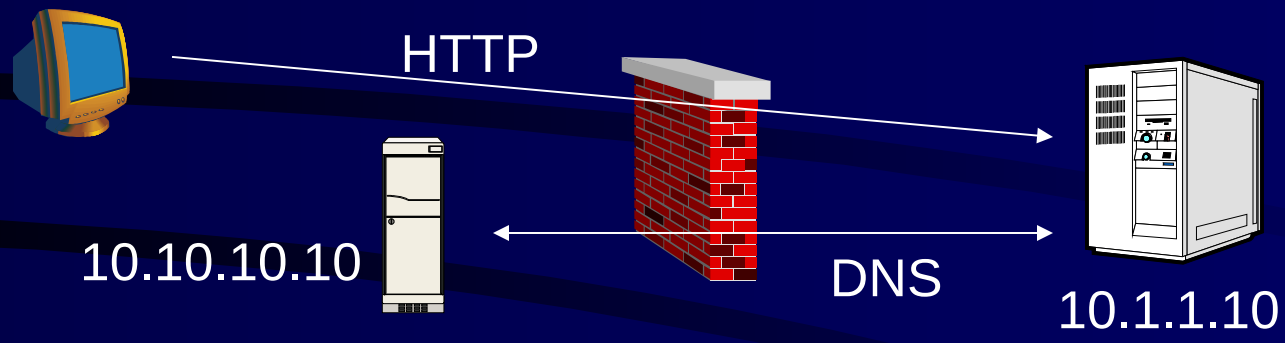
Bezstavový firewall



Action	Proto	Source	Destination	Service	
permit	TCP	ANY	ANY	ANY	! SYN
permit	TCP	ANY	10.1.1.10	http(80)	
permit	ICMP	ANY	ANY		
permit	UDP	10.10.10.10	10.1.1.10	dns(53)	
permit	UDP	10.1.1.10	10.10.10.10	dns(53)	
deny	ANY	ANY	ANY		

Filtrovacie pravidlá

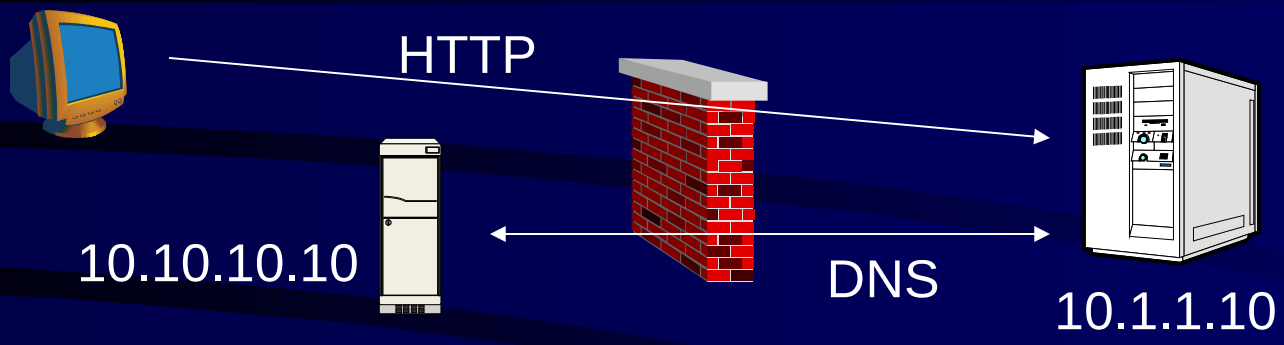
Stavový firewall



Action	Proto	Source	Destination	Service
permit	TCP	ANY	10.1.1.10	http(80)
permit	ICMP	ANY	ANY	echo
permit	UDP	10.1.1.10	10.10.10.10	dns(53)
deny	ANY	ANY	ANY	

Filtrovacie pravidlá

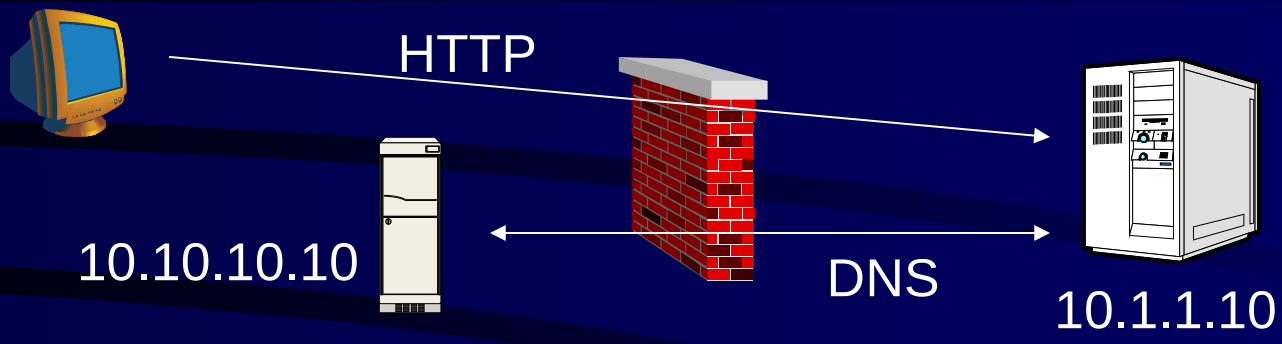
Linux ipchains




```
ipchains -P forward DENY
ipchains -A forward -p tcp ! -y -j ACCEPT
ipchains -A forward -p tcp -d 10.1.1.10 80 -j ACCEPT
ipchains -A forward -p icmp -j ACCEPT
ipchains -A forward -p udp -s 10.10.10.10 -d 10.1.1.10 53 -j ACCEPT
ipchains -A forward -p udp -s 10.1.1.10 -d 10.10.10.10 53 -j ACCEPT
```

Filtrovacie pravidlá

Cisco ACL




```
ip access-list 111 permit tcp any any established
ip access-list 111 permit any host 10.1.1.10 eq 80
ip access-list 111 permit icmp any any
ip access-list 111 permit udp host 10.10.10.10 host 10.1.1.10 eq 53
ip access-list 111 permit udp host 10.1.1.10 host 10.10.10.10 eq 53
ip access-list 111 deny ip any any

ip access-group 111 out
```

Linux firewalling

- 2.0.x - “ipfwadm”
  - Len základné funkcie bezstavového firewallu, nízka rozšíriteľnosť
- 2.2.x - ipchains
  - Rozšírená funkčnosť, integrované možnosti “masquerading” a “transparent proxy”, stále nízka rozšíriteľnosť
- 2.4.x - netfilter
  - Flexibilná kostra pre integráciu firewallingu do služieb sieťových protokolov v jadre
  - Bohaté možnosti, ľahké rozširovanie

Ďakujem za pozornosť

Ing. Radovan Semančík
semancik@bgs.sk