Grundlagen Informationsicherheit und Datensicherheit, Blatt 4

Lukas Baur, 3131138
Felix Bühler, 2973410
Marco Hildenbrand, 3137242

17. Dezember 2017

Problem 1: BGP

(a)

In our case: if paths have the same length, we will use the one with lower AS-number.

Tabelle 1: AS1

AS	IP	via
1	1.2.3.0/24 17.9.8.0/25	-
2	5.2.0.0/16	AS2
3	92.18.2.0/24	AS3
4	18.2.1.0/26	AS2, AS4
5	80.90.42.0/24	AS2, AS4, AS5
6	15.23.2.0/24	AS3, AS6

Tabelle 2: AS2

AS	IP	via
1	1.2.3.0/24 17.9.8.0/25	AS1
2	5.2.0.0/16	-
3	92.18.2.0/24	AS3
4	18.2.1.0/26	AS4
5	80.90.42.0/24	AS4, AS5
6	15.23.2.0/24	AS3, AS6

Tabelle 3: AS3

AS	IP	via
1	1.2.3.0/24 17.9.8.0/25	AS1
2	5.2.0.0/16	AS2
3	92.18.2.0/24	-
4	18.2.1.0/26	AS4
5	80.90.42.0/24	AS4, AS5
6	15.23.2.0/24	AS6

Tabelle 4: AS4

AS	IP	via
1	1.2.3.0/24 17.9.8.0/25	AS2, AS1
2	5.2.0.0/16	AS2
3	92.18.2.0/24	AS3
4	18.2.1.0/26	-
5	80.90.42.0/24	AS5
6	15.23.2.0/24	AS6

Tabelle 5: AS5

AS	IP	via
1	1.2.3.0/24 17.9.8.0/25	AS4, AS2, AS1
2	5.2.0.0/16	AS4, AS2
3	92.18.2.0/24	AS4, AS3
4	18.2.1.0/26	AS4
5	80.90.42.0/24	-
6	15.23.2.0/24	AS6

Tabelle 6: AS6

AS	IP	via
1	1.2.3.0/24 17.9.8.0/25	AS3, AS1
2	5.2.0.0/16	AS3, AS2
3	92.18.2.0/24	AS3
4	18.2.1.0/26	AS4
5	80.90.42.0/24	AS5
6	15.23.2.0/24	-

(b)

Only showing the changed tables. Changes are underlined.

Tabelle 7: AS4'

AS	IP	via
1	~~1.2.3.0/24~~ 17.9.8.0/25	AS2, AS1
2	5.2.0.0/16	AS2
3	92.18.2.0/24	AS3
4	18.2.1.0/26	-
5	80.90.42.0/24 1.2.3.0/24	AS5
6	15.23.2.0/24	AS6

Tabelle 8: AS5’

AS	IP	via
1	~~1.2.3.0/24~~ 17.9.8.0/25	AS4, AS2, AS1
2	5.2.0.0/16	AS4, AS2
3	92.18.2.0/24	AS4, AS3
4	18.2.1.0/26	AS4
5	80.90.42.0/24 1.2.3.0/24	AS5
6	15.23.2.0/24	AS6

Tabelle 9: AS6’

AS	IP	via
1	~~1.2.3.0/24~~ 17.9.8.0/25	AS3, AS1
2	5.2.0.0/16	AS3, AS2
3	92.18.2.0/24	AS3
4	18.2.1.0/26	AS4
5	80.90.42.0/24 1.2.3.0/24	AS5
6	15.23.2.0/24	-

Problem 2: Network Trace

(a)

a

(b)

a

Problem 3: Probability of Successful DNS Spoofing

(a)

- the original DNS request (needs to be repeated in the response)
- the IP address of the DNS server (the sender address of response)

- the DNS transaction ID (TXID)
- the UDP/TCP source port number that Alice used
- (if TCP is used, the TCP sequence number)

The attaker could know the 'oridignal DNS request' and the 'IP of the DNS server'.

What he has to guess:

- #TXIDs = 16 Bits = 65536 possibilities
- #Ports = 16 Bits = 65536 possibilities
  (usually many ports are already blocked if they are too low)
- (#TCP-Sequence-numbers = 16 Bits = 65536)
  (usually dns is done over udp)

UDP: $\frac{1}{65536} * \frac{1}{65536} = \frac{1}{4294967296} = 2.3283064 * 10^{-10}$

TCP: $\frac{1}{65536} * \frac{1}{65536} * \frac{1}{65536} = \frac{1}{2.8147498*10^{14}} = 3.5527136 * 10^{-15}$

(b)

$\frac{2000}{65536} = \frac{125}{4096}$

$0.5 = \frac{125}{4096-(X*125)}$

$X = 30.768$

On average the attacker successes after 62000 requests, 31 rounds (=3.1 seconds).