isec 2024: Fragestunde

W50

Netzsicherheit

Diese Woche:

— Angriffe auf das Netz
— Nutzung des Netzes zur Entschärfung von Angriffen auf Software ("Firewalls")

Anderes Thema (nicht diese Woche):

— Sicherheit von Menschen beim Benutzen des Netzes

Software im Netz

Besondere Gefährdung: sitting duck

- Angreifer kann jederzeit aktiv werden, über längere Zeit
- Angreifer kann immer wieder neue Angriffe probieren

— Netz kann gegen Angriffe auf Software helfen

— Netz selbst wird so zum lohnenderen Angriffsziel

Angriffe auf das Netz: nach OSI-Schichten

- L1: Abhören, Verändern, Einschleusen, Unterdrücken
  - erfordert Kontakt mit physischen Medium
- L2/L3:
  - Forwarding/Routing verwirren ➔ Fern-Zugriff auf Abhören, Verändern, Einschleusen, Unterdrücken
  - Scannen (IPv4, Hinweise nutzen für IPv6)
- L4: Stören (z.B. RST-Angriffe), Überlasten (z.B. SYN-Flooding)
- L7: Betriebsprotokolle (z.B. DNS), Anwendungen

Angriffsmechanismen und deren Abwehr

- On-Path-Angreifer: kann
  Abhören, Verändern, Einschleusen, Unterdrücken
  ➔ Umleitungen erschweren
- Identitätsbehauptungen fälschen
  ➔ Authentisierung! (kryptographisch gegen Abhören)
  - Ende-zu-Ende, gegenseitig?

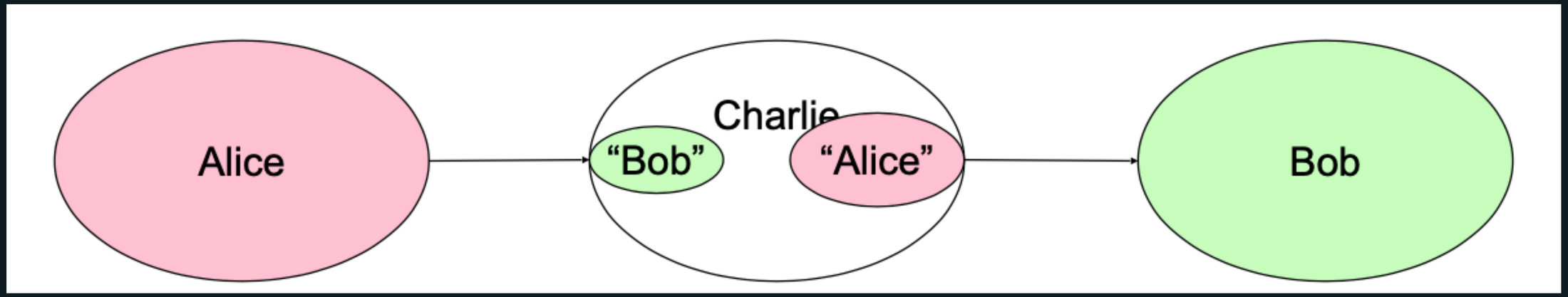
Das Internet-Bedrohungsmodell

Dolev-Yao threat model, 1983:

- Netz ist vollständig kompromittiert, Angreifer kann Abhören, Verändern, Einschleusen, Unterdrücken
- Endsysteme hingegen als sicher angenommen
  - Folgen mindern: z.B. "perfect" forward secrecy
  - Überprüfen: Attestierung

Terminologie: Angriffe (1)

— passive, aktive Angriffe
— off-path, on-path
— Machine-in-the-middle (MITM)-Angriffe



Terminologie: Angriffe (2)

DoS-Angriffe, DDoS
Amplification (Verstärker-Angriffe)

Verbreitung:
- Wurm (z.B. Slammer)
- Angriffe via Botnets

Internet Background Radiation

***Firewalls** are the **network** response to a **host** security problem*

The primary purpose of firewalls has always been to shield buggy code from bad guys.

— Steve Bellovin, IAB (1996–2002) IETF Security AD (2002–2004)

Terminologie: Firewalls

- Paketfilter
  - Firewall-Regeln (5-Tupel: Protokoll (TCP/UDP/...), IP-Adresse/Port × Source/Destination)
  - SPI (Stateful Packet Inspection)
- Application Layer Gateway (Proxy)
- DMZ (Grenznetz: ALGs beschützt von Paketfiltern)
- Kein Firewall: NAT (Network Address[/Port] Translation)
- "Firewall-friendly"; ➔ alles über HTTP(S)

traceroute

```
rodie [/]$ traceroute 134.102.201.17
traceroute to 134.102.201.17 (134.102.201.17), 64 hops max, 52 byte packets
 1  134.102.3.190 (134.102.3.190)  23.715 ms  38.004 ms  27.015 ms
 2  fb3-c4500x-po3.noc.uni-bremen.de (134.102.0.38)  23.646 ms  65.238 ms  26.24
3 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * *^C
rodie 130[/]$
```

```
rodie [/]$ traceroute 134.102.201.17
traceroute to 134.102.201.17 (134.102.201.17), 64 hops max, 52 byte packets
 1  192.168.217.1 (192.168.217.1)  4.870 ms  4.085 ms  3.207 ms
 2  speedport.ip (192.168.2.1)  4.731 ms  3.988 ms  4.714 ms
 3  p3e9bf2fd.dip0.t-ipconnect.de (62.155.242.253)  8.705 ms  8.667 ms  8.951 ms
 4  d-ed6-i.d.de.net.dtag.de (217.5.119.66)  16.215 ms
    d-ed6-i.d.de.net.dtag.de (217.5.119.74)  16.485 ms
    d-ed6-i.d.de.net.dtag.de (217.5.119.66)  17.403 ms
 5  193.159.165.115 (193.159.165.115)  21.308 ms  22.485 ms  22.390 ms
 6  kr-bre66-0.x-win.dfn.de (188.1.244.190)  22.122 ms  21.802 ms  22.618 ms
 7  v9600-po1.noc.uni-bremen.de (134.102.0.98)  22.920 ms  23.584 ms  30.138 ms
 8  fb3-c4500x-po3.noc.uni-bremen.de (134.102.0.38)  89.957 ms  87.953 ms  57.59
1 ms
 9  * * *
10  * * *
11  * *
```

```
rodie [/]$ traceroute 134.102.201.17
traceroute to 134.102.201.17 (134.102.201.17), 64 hops max, 52 byte packets
 1  v-74-91-112-207.unman-vds.inap-atlanta.nfoservers.com (74.91.112.207)  122.1
87 ms  123.403 ms  122.775 ms
 2  router.inap-atlanta.nfoservers.com (192.223.28.253)  121.864 ms  122.198 ms
 122.279 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * *^C
rodie 130[/]$
```

```
rodie [/]$ traceroute 134.102.201.17
traceroute to 134.102.201.17 (134.102.201.17), 64 hops max, 52 byte packets
 1  seaexportchina.com (111.90.149.156)  194.686 ms  192.570 ms  191.639 ms
 2  server1.kamon.la (111.90.149.2)  193.510 ms  194.734 ms  209.011 ms
 3  * * *
 4  111.90.138.181 (111.90.138.181)  194.256 ms  194.898 ms  193.446 ms
 5  dyn189-b100-access.superdsl.com.sg (202.83.100.189)  200.318 ms  201.326 ms
 200.600 ms
 6  132.147.112.109 (132.147.112.109)  200.246 ms  200.440 ms  200.487 ms
 7  e0-1.switch2.sin1.he.net (27.50.33.93)  200.821 ms * *
 8  * * *
 9  * * *
10  * * port-channel10.core3.fra1.he.net (72.52.92.69)  468.265 ms
11  cr-fra2-be1.x-win.dfn.de (80.81.192.222)  349.644 ms  386.229 ms
    cr-erl2-be1.x-win.dfn.de (80.81.193.222)  354.164 ms
12  cr-han2-be6.x-win.dfn.de (188.1.144.134)  354.915 ms
    cr-tub2-be10.x-win.dfn.de (188.1.146.210)  363.452 ms  365.325 ms
13  kr-bre66-0.x-win.dfn.de (188.1.244.190)  358.173 ms
    cr-han2-be7.x-win.dfn.de (188.1.144.137)  363.568 ms
    kr-bre66-0.x-win.dfn.de (188.1.244.190)  356.428 ms
14  vcr-po1.noc.uni-bremen.de (134.102.0.98)  396.494 ms
    kr-bre66-0.x-win.dfn.de (188.1.244.190)  363.949 ms
    vcr-po1.noc.uni-bremen.de (134.102.0.98)  360.758 ms
15  vcr-po1.noc.uni-bremen.de (134.102.0.98)  403.789 ms  385.854 ms
    fb3-c4500x-po3.noc.uni-bremen.de (134.102.0.38)  390.341 ms
```