SWP 21 - Gruppe 01: Abwehr von Denial-of-Service-Angriffen durch effiziente User-Space Paketverarbeitung

Abschlussveranstaltung

21. Juli 2021

Technische Universität Ilmenau

Das Problem DDoS[3]

[3] DDoS = Distributed Denial of Service

Das Problem DDoS[3]

Einfach und beliebt

[3] DDoS = Distributed Denial of Service

Das Problem DDoS[3]

Einfach und beliebt

Fast unaufhaltsam

[3] DDoS = Distributed Denial of Service

Das Problem DDoS[3]

Einfach und beliebt

Fast unaufhaltsam

Abwehr komplex und ressourcenintensiv

[3] DDoS = Distributed Denial of Service

Das Problem DDoS[3]

Einfach und beliebt

Fast unaufhaltsam

Abwehr komplex und ressourcenintensiv

Angriffsvolumen verdoppelt mindestens jährlich [1]

[1] ns-cdn.neustar.biz

[3] DDoS = Distributed Denial of Service

Das Problem DDoS[3]

Einfach und beliebt

Fast unaufhaltsam

Abwehr komplex und ressourcenintensiv

Angriffsvolumen verdoppelt mindestens jährlich [1]

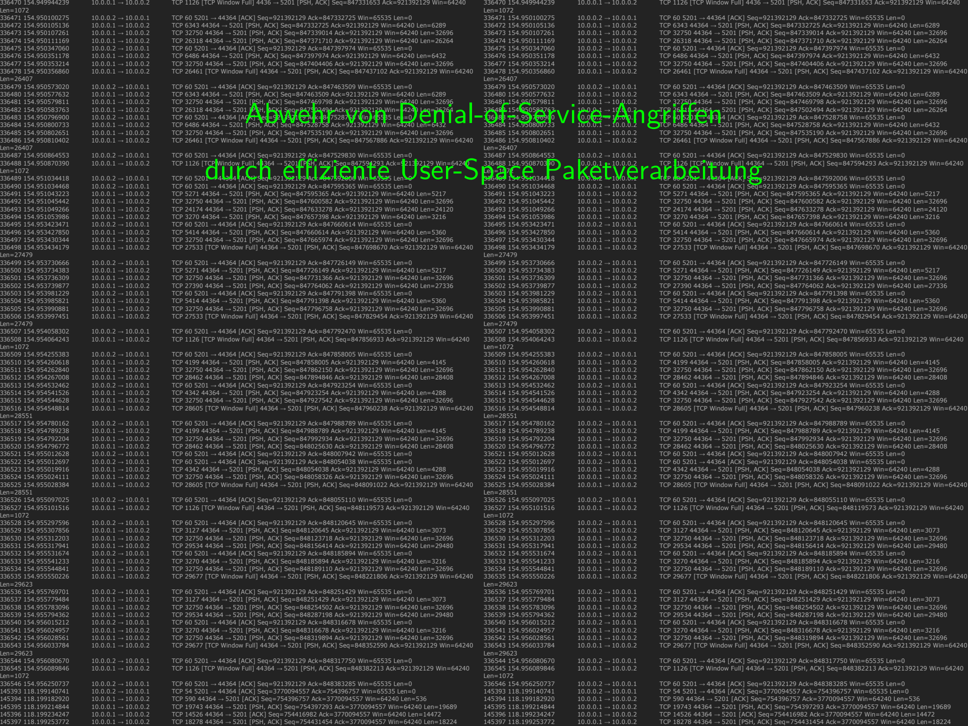
Schäden bei ∼323.400 Euro je Stunde [2]

[1] ns-cdn.neustar.biz

[2] https://it-service.network

[3] DDoS = Distributed Denial of Service

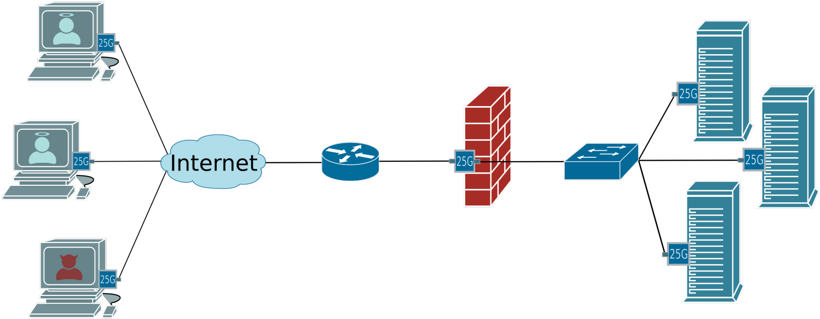
Abwehr von Denial-of-Service-Angriffen durch effiziente User-Space Paketverarbeitung



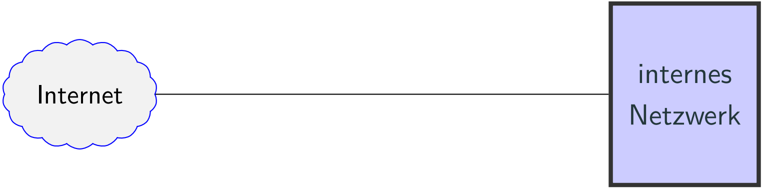
```
336470 154.949944239    10.0.0.1 → 10.0.0.2    TCP 1126 [TCP Window Full] 4436 → 5201 [PSH, ACK] Seq=847331653 Ack=921392129 Win=64240
Len=1072
336471 154.950100275    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=847332725 Win=65535 Len=0
336472 154.950105136    10.0.0.1 → 10.0.0.2    TCP 6343 44364 → 5201 [PSH, ACK] Seq=847332725 Ack=921392129 Win=64240 Len=6289
336473 154.950107261    10.0.0.1 → 10.0.0.2    TCP 32750 44364 → 5201 [PSH, ACK] Seq=847339014 Ack=921392129 Win=64240 Len=32696
336474 154.950111169    10.0.0.1 → 10.0.0.2    TCP 26318 44364 → 5201 [PSH, ACK] Seq=847371710 Ack=921392129 Win=64240 Len=26264
336475 154.950347060    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=847397974 Win=65535 Len=0
336476 154.950351178    10.0.0.1 → 10.0.0.2    TCP 6486 44364 → 5201 [PSH, ACK] Seq=847397974 Ack=921392129 Win=64240 Len=6432
336477 154.950353214    10.0.0.1 → 10.0.0.2    TCP 32750 44364 → 5201 [PSH, ACK] Seq=847404406 Ack=921392129 Win=64240 Len=32696
336478 154.950356860    10.0.0.1 → 10.0.0.2    TCP 26461 [TCP Window Full] 44364 → 5201 [PSH, ACK] Seq=847437102 Ack=921392129 Win=64240
Len=26407
336479 154.950573020    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=847463509 Win=65535 Len=0
336480 154.950577632    10.0.0.1 → 10.0.0.2    TCP 6343 44364 → 5201 [PSH, ACK] Seq=847463509 Ack=921392129 Win=64240 Len=6289
336481 154.950579811    10.0.0.1 → 10.0.0.2    TCP 32750 44364 → 5201 [PSH, ACK] Seq=847469798 Ack=921392129 Win=64240 Len=32696
336482 154.950583763    10.0.0.1 → 10.0.0.2    TCP 26318 44364 → 5201 [PSH, ACK] Seq=847502494 Ack=921392129 Win=64240 Len=26264
336483 154.950796900    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=847528758 Win=65535 Len=0
336484 154.950800733    10.0.0.1 → 10.0.0.2    TCP 6486 44364 → 5201 [PSH, ACK] Seq=847528758 Ack=921392129 Win=64240 Len=6432
336485 154.950802651    10.0.0.1 → 10.0.0.2    TCP 32750 44364 → 5201 [PSH, ACK] Seq=847535190 Ack=921392129 Win=64240 Len=32696
336486 154.950810402    10.0.0.1 → 10.0.0.2    TCP 26461 [TCP Window Full] 44364 → 5201 [PSH, ACK] Seq=847567886 Ack=921392129 Win=64240
Len=26407
336487 154.950864553    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=847529830 Win=65535 Len=0
336488 154.950870390    10.0.0.1 → 10.0.0.2    TCP 1126 [TCP Window Full] 44364 → 5201 [PSH, ACK] Seq=847594293 Ack=921392129 Win=64240
Len=1072
336489 154.951034418    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=847592006 Win=65535 Len=0
336490 154.951034468    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=847595365 Win=65535 Len=0
336491 154.951043223    10.0.0.1 → 10.0.0.2    TCP 5271 44364 → 5201 [PSH, ACK] Seq=847595365 Ack=921392129 Win=64240 Len=5217
336492 154.951045442    10.0.0.1 → 10.0.0.2    TCP 32750 44364 → 5201 [PSH, ACK] Seq=847600582 Ack=921392129 Win=64240 Len=32696
336493 154.951049266    10.0.0.1 → 10.0.0.2    TCP 24174 44364 → 5201 [PSH, ACK] Seq=847633278 Ack=921392129 Win=64240 Len=24120
336494 154.951053986    10.0.0.1 → 10.0.0.2    TCP 3270 44364 → 5201 [PSH, ACK] Seq=847657398 Ack=921392129 Win=64240 Len=3216
336495 154.953423471    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=847660614 Win=65535 Len=0
336496 154.953427850    10.0.0.1 → 10.0.0.2    TCP 5414 44364 → 5201 [PSH, ACK] Seq=847660614 Ack=921392129 Win=64240 Len=5360
336497 154.953430344    10.0.0.1 → 10.0.0.2    TCP 32750 44364 → 5201 [PSH, ACK] Seq=847665974 Ack=921392129 Win=64240 Len=32696
336498 154.953434179    10.0.0.1 → 10.0.0.2    TCP 27533 [TCP Window Full] 44364 → 5201 [PSH, ACK] Seq=847698670 Ack=921392129 Win=64240
Len=27479
336499 154.953730666    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=847726149 Win=65535 Len=0
336500 154.953734383    10.0.0.1 → 10.0.0.2    TCP 5271 44364 → 5201 [PSH, ACK] Seq=847726149 Ack=921392129 Win=64240 Len=5217
336501 154.953736309    10.0.0.1 → 10.0.0.2    TCP 32750 44364 → 5201 [PSH, ACK] Seq=847731366 Ack=921392129 Win=64240 Len=32696
336502 154.953739877    10.0.0.1 → 10.0.0.2    TCP 27390 44364 → 5201 [PSH, ACK] Seq=847764062 Ack=921392129 Win=64240 Len=27336
336503 154.953981229    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=847791398 Win=65535 Len=0
336504 154.953985821    10.0.0.1 → 10.0.0.2    TCP 5414 44364 → 5201 [PSH, ACK] Seq=847791398 Ack=921392129 Win=64240 Len=5360
336505 154.953990881    10.0.0.1 → 10.0.0.2    TCP 32750 44364 → 5201 [PSH, ACK] Seq=847796758 Ack=921392129 Win=64240 Len=32696
336506 154.953997451    10.0.0.1 → 10.0.0.2    TCP 27533 [TCP Window Full] 44364 → 5201 [PSH, ACK] Seq=847829454 Ack=921392129 Win=64240
Len=27479
336507 154.954058302    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=847792470 Win=65535 Len=0
336508 154.954064243    10.0.0.1 → 10.0.0.2    TCP 1126 [TCP Window Full] 44364 → 5201 [PSH, ACK] Seq=847856933 Ack=921392129 Win=64240
Len=1072
336509 154.954255383    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=847858005 Win=65535 Len=0
336510 154.954260618    10.0.0.1 → 10.0.0.2    TCP 4199 44364 → 5201 [PSH, ACK] Seq=847858005 Ack=921392129 Win=64240 Len=4145
336511 154.954262840    10.0.0.1 → 10.0.0.2    TCP 32750 44364 → 5201 [PSH, ACK] Seq=847862150 Ack=921392129 Win=64240 Len=32696
336512 154.954267008    10.0.0.1 → 10.0.0.2    TCP 28462 44364 → 5201 [PSH, ACK] Seq=847894846 Ack=921392129 Win=64240 Len=28408
336513 154.954532462    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=847923254 Win=65535 Len=0
336514 154.954541526    10.0.0.1 → 10.0.0.2    TCP 4342 44364 → 5201 [PSH, ACK] Seq=847923254 Ack=921392129 Win=64240 Len=4288
336515 154.954544628    10.0.0.1 → 10.0.0.2    TCP 32750 44364 → 5201 [PSH, ACK] Seq=847927542 Ack=921392129 Win=64240 Len=32696
336516 154.954548814    10.0.0.1 → 10.0.0.2    TCP 28605 [TCP Window Full] 44364 → 5201 [PSH, ACK] Seq=847960238 Ack=921392129 Win=64240
Len=28551
336517 154.954780162    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=847988789 Win=65535 Len=0
336518 154.954789238    10.0.0.1 → 10.0.0.2    TCP 4199 44364 → 5201 [PSH, ACK] Seq=847988789 Ack=921392129 Win=64240 Len=4145
336519 154.954792204    10.0.0.1 → 10.0.0.2    TCP 32750 44364 → 5201 [PSH, ACK] Seq=847992934 Ack=921392129 Win=64240 Len=32696
336520 154.954796772    10.0.0.1 → 10.0.0.2    TCP 28462 44364 → 5201 [PSH, ACK] Seq=848025630 Ack=921392129 Win=64240 Len=28408
336521 154.955012628    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=848007942 Win=65535 Len=0
336522 154.955012697    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=848054038 Win=65535 Len=0
336523 154.955019916    10.0.0.1 → 10.0.0.2    TCP 4342 44364 → 5201 [PSH, ACK] Seq=848054038 Ack=921392129 Win=64240 Len=4288
336524 154.955024111    10.0.0.1 → 10.0.0.2    TCP 32750 44364 → 5201 [PSH, ACK] Seq=848058326 Ack=921392129 Win=64240 Len=32696
336525 154.955028384    10.0.0.1 → 10.0.0.2    TCP 28605 [TCP Window Full] 44364 → 5201 [PSH, ACK] Seq=848091022 Ack=921392129 Win=64240
Len=28551
336526 154.955097025    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=848055110 Win=65535 Len=0
336527 154.955101516    10.0.0.1 → 10.0.0.2    TCP 1126 [TCP Window Full] 44364 → 5201 [PSH, ACK] Seq=848119573 Ack=921392129 Win=64240
Len=1072
336528 154.955297596    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=848120645 Win=65535 Len=0
336529 154.955307856    10.0.0.1 → 10.0.0.2    TCP 3127 44364 → 5201 [PSH, ACK] Seq=848120645 Ack=921392129 Win=64240 Len=3073
336530 154.955312203    10.0.0.1 → 10.0.0.2    TCP 32750 44364 → 5201 [PSH, ACK] Seq=848123718 Ack=921392129 Win=64240 Len=32696
336531 154.955317941    10.0.0.1 → 10.0.0.2    TCP 29534 44364 → 5201 [PSH, ACK] Seq=848156414 Ack=921392129 Win=64240 Len=29480
336532 154.955531674    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=848185894 Win=65535 Len=0
336533 154.955541233    10.0.0.1 → 10.0.0.2    TCP 3270 44364 → 5201 [PSH, ACK] Seq=848185894 Ack=921392129 Win=64240 Len=3216
336534 154.955544841    10.0.0.1 → 10.0.0.2    TCP 32750 44364 → 5201 [PSH, ACK] Seq=848189110 Ack=921392129 Win=64240 Len=32696
336535 154.955550226    10.0.0.1 → 10.0.0.2    TCP 29677 [TCP Window Full] 44364 → 5201 [PSH, ACK] Seq=848221806 Ack=921392129 Win=64240
Len=29623
336536 154.955769701    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=848251429 Win=65535 Len=0
336537 154.955779484    10.0.0.1 → 10.0.0.2    TCP 3127 44364 → 5201 [PSH, ACK] Seq=848251429 Ack=921392129 Win=64240 Len=3073
336538 154.955783096    10.0.0.1 → 10.0.0.2    TCP 32750 44364 → 5201 [PSH, ACK] Seq=848254502 Ack=921392129 Win=64240 Len=32696
336539 154.955794362    10.0.0.1 → 10.0.0.2    TCP 29534 44364 → 5201 [PSH, ACK] Seq=848287198 Ack=921392129 Win=64240 Len=29480
336540 154.956015212    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=848316678 Win=65535 Len=0
336541 154.956024957    10.0.0.1 → 10.0.0.2    TCP 3270 44364 → 5201 [PSH, ACK] Seq=848316678 Ack=921392129 Win=64240 Len=3216
336542 154.956028561    10.0.0.1 → 10.0.0.2    TCP 32750 44364 → 5201 [PSH, ACK] Seq=848319894 Ack=921392129 Win=64240 Len=32696
336543 154.956033784    10.0.0.1 → 10.0.0.2    TCP 29677 [TCP Window Full] 44364 → 5201 [PSH, ACK] Seq=848352590 Ack=921392129 Win=64240
Len=29623
336544 154.956080670    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=848317750 Win=65535 Len=0
336545 154.956089846    10.0.0.1 → 10.0.0.2    TCP 1126 [TCP Window Full] 44364 → 5201 [PSH, ACK] Seq=848382213 Ack=921392129 Win=64240
Len=1072
336546 154.956250737    10.0.0.2 → 10.0.0.1    TCP 60 5201 → 44364 [ACK] Seq=921392129 Ack=848383285 Win=65535 Len=0
145393 118.199140741    10.0.0.2 → 10.0.0.1    TCP 54 5201 → 44364 [ACK] Seq=3770094557 Ack=754396757 Win=65535 Len=0
145394 118.199182920    10.0.0.1 → 10.0.0.2    TCP 590 44364 → 5201 [ACK] Seq=754396757 Ack=3770094557 Win=64240 Len=536
145395 118.199214844    10.0.0.1 → 10.0.0.2    TCP 19743 44364 → 5201 [PSH, ACK] Seq=754397293 Ack=3770094557 Win=64240 Len=19689
145396 118.199234247    10.0.0.1 → 10.0.0.2    TCP 14526 44364 → 5201 [ACK] Seq=754416982 Ack=3770094557 Win=64240 Len=14472
145397 118.199253772    10.0.0.1 → 10.0.0.2    TCP 18278 44364 → 5201 [PSH, ACK] Seq=754431454 Ack=3770094557 Win=64240 Len=18224
```

Abwehr von Denial-of-Service-Angriffen durch effiziente User-Space Paketverarbeitung

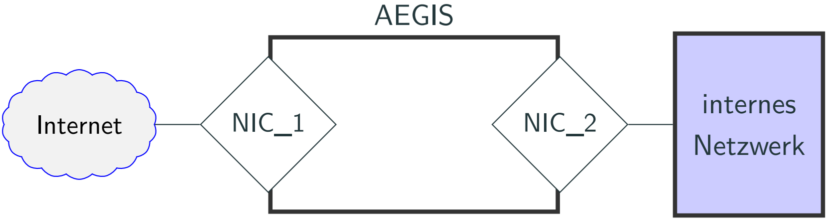
Wie funktioniert AEGIS?



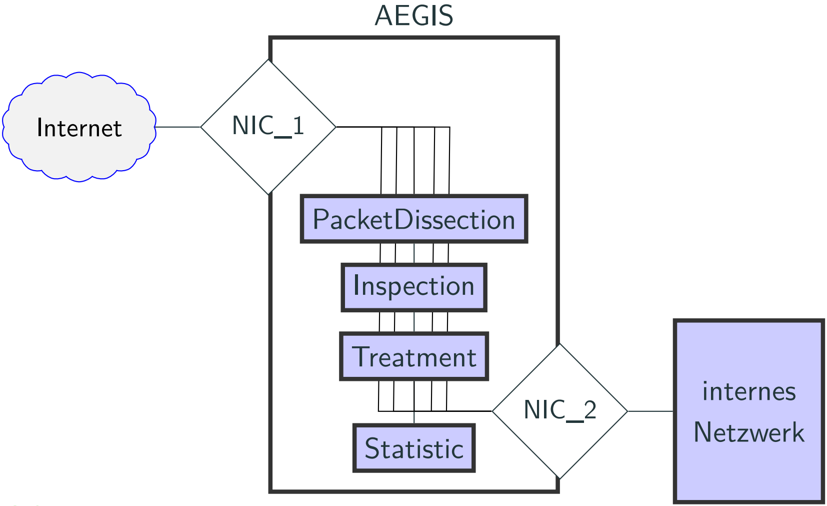
Wie funktioniert AEGIS?



Wie funktioniert AEGIS?



Wie funktioniert AEGIS?



Was kann AEGIS?

□ Abwehr von SYN Flood Attacken

□ Abwehr von SYN-FIN/SYN-FIN-ACK Attacken

□ Datenrate $\geq$ 5 Gbit/s [4]; Paketrate $\geq$ 7 Mpps [5]

□ Konfiguration durch Nutzer

□ Skalieren

[4] Gigabit per second

[5] Million packages per second

Was kann AEGIS?

- ☑ Abwehr von SYN Flood Attacken
- □ Abwehr von SYN-FIN/SYN-FIN-ACK Attacken
- □ Datenrate $\geq$ 5 Gbit/s [4]; Paketrate $\geq$ 7 Mpps [5]
- □ Konfiguration durch Nutzer
- □ Skalieren

[4] Gigabit per second

[5] Million packages per second

Was kann AEGIS?

- ☑ Abwehr von SYN Flood Attacken
- ☑ Abwehr von SYN-FIN/SYN-FIN-ACK Attacken
- □ Datenrate $\geq$ 5 Gbit/s [4]; Paketrate $\geq$ 7 Mpps [5]
- □ Konfiguration durch Nutzer
- □ Skalieren

[4] Gigabit per second

[5] Million packages per second

Was kann AEGIS?

- ☑ Abwehr von SYN Flood Attacken
- ☑ Abwehr von SYN-FIN/SYN-FIN-ACK Attacken
- ☑ Datenrate $\geq$ 5 Gbit/s [4]; Paketrate $\geq$ 7 Mpps [5]
- □ Konfiguration durch Nutzer
- □ Skalieren

[4] Gigabit per second

[5] Million packages per second

Was kann AEGIS?

- ☑ Abwehr von SYN Flood Attacken
- ☑ Abwehr von SYN-FIN/SYN-FIN-ACK Attacken
- ☑ Datenrate $\geq$ 5 Gbit/s [4]; Paketrate $\geq$ 7 Mpps [5]
- ☑ Konfiguration durch Nutzer
- □ Skalieren

[4] Gigabit per second

[5] Million packages per second

Was kann AEGIS?

☑ Abwehr von SYN Flood Attacken

☑ Abwehr von SYN-FIN/SYN-FIN-ACK Attacken

☑ Datenrate $\geq$ 5 Gbit/s [4]; Paketrate $\geq$ 7 Mpps [5]

☑ Konfiguration durch Nutzer

☑ Skalieren

[4] Gigabit per second

[5] Million packages per second

Was kostet AEGIS?

- Leistungsfähiger Rechner mit Multicore CPU

Was kostet AEGIS?

□ Leistungsfähiger Rechner mit Multicore CPU

□ DPDK-fähige Netzwerkkarte

Was kostet AEGIS?

□ Leistungsfähiger Rechner mit Multicore CPU

□ DPDK-fähige Netzwerkkarte

□ Stromkosten von $\sim$1000€ p.a.

Was kostet AEGIS?

☐ Leistungsfähiger Rechner mit Multicore CPU

☐ DPDK-fähige Netzwerkkarte

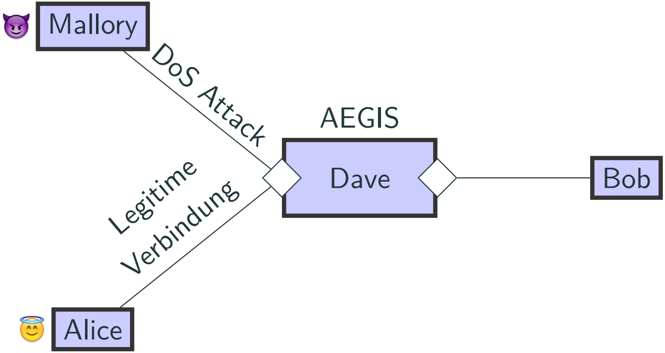
☐ Stromkosten von ∼1000€ p.a.

☐ Delay für Verbindungen aus dem internen Netz: 0%

Was kostet AEGIS?

- □ Leistungsfähiger Rechner mit Multicore CPU
- □ DPDK-fähige Netzwerkkarte
- □ Stromkosten von $\sim$1000€ p.a.
- □ Delay für Verbindungen aus dem internen Netz: 0%
- □ Delay für Verbindungen aus dem externen Netz: $<$ 30%

Der Testaufbau



Herausforderungen

□ Isolation vom Internet durch Network-Namespaces

Herausforderungen

□ Isolation vom Internet durch Network-Namespaces

□ Nachbau der DPDK-Library für Unit-Tests

Herausforderungen

□ Isolation vom Internet durch Network-Namespaces

□ Nachbau der DPDK-Library für Unit-Tests

□ Begrenzte Hardwareressourcen des Testbeds

Herausforderungen

- □ Isolation vom Internet durch Network-Namespaces
- □ Nachbau der DPDK-Library für Unit-Tests
- □ Begrenzte Hardwareressourcen des Testbeds
- □ Codeeffizienz als maßgebliches Erfolgskriterium

Herausforderungen

□ Isolation vom Internet durch Network-Namespaces

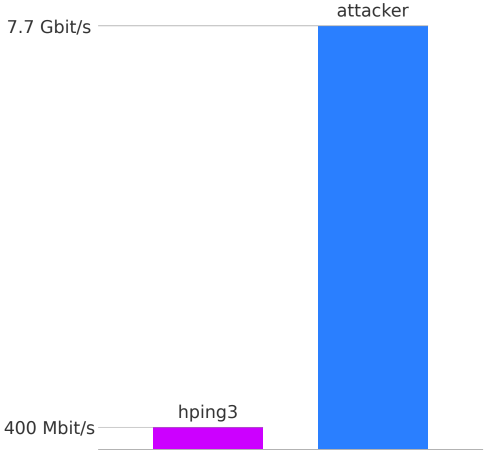
□ Nachbau der DPDK-Library für Unit-Tests

□ Begrenzte Hardwareressourcen des Testbeds

□ Codeeffizienz als maßgebliches Erfolgskriterium

□ Notwendigkeit der Entwicklung eigener Angriffstools

Der Angreifer



Live aus dem Labor

Bewertung des Softwareprojekts

Aus Umfragen ergab sich:

Bewertung des Softwareprojekts

Aus Umfragen ergab sich:

- 😀 Praxiserfahrung

Bewertung des Softwareprojekts

Aus Umfragen ergab sich:

- 😀 Praxiserfahrung
- 😀 Teamarbeit

Bewertung des Softwareprojekts

Aus Umfragen ergab sich:

- 😀 Praxiserfahrung
- 😀 Teamarbeit
- 😀 Team Programming

Bewertung des Softwareprojekts

Aus Umfragen ergab sich:

- 😀 Praxiserfahrung
- 😀 Teamarbeit
- 😀 Team Programming
- 😵 Bewältigung komplexer Aufgabenstellungen

Bewertung des Softwareprojekts

Aus Umfragen ergab sich:

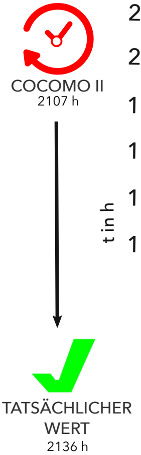
- 😀 Praxiserfahrung
- 😀 Teamarbeit
- 😀 Team Programming
- 😵 Bewältigung komplexer Aufgabenstellungen
- 😀 Erfahrungen mit Git, LaTeX, Linux und DPDK

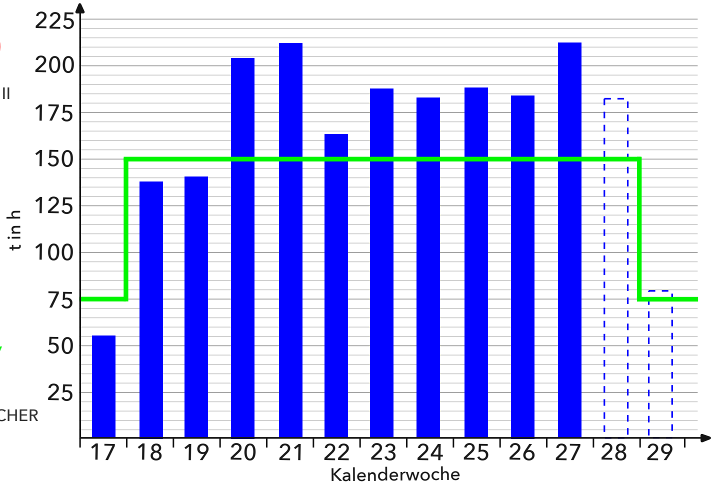
Bewertung des Softwareprojekts

Aus Umfragen ergab sich:

- 😀 Praxiserfahrung
- 😀 Teamarbeit
- 😀 Team Programming
- 😵 Bewältigung komplexer Aufgabenstellungen
- 😀 Erfahrungen mit Git, LaTeX, Linux und DPDK
- 😎 Ambitionen zur Projektfortführung

Projekt Zeitrahmen





Zukunftsvisionen

EGIS

Zukunftsvisionen

□ Repository auf Github

Zukunftsvisionen

- □ Repository auf Github
- □ Erweiterung der Abwehrmechanismen

Zukunftsvisionen

- □ Repository auf Github
- □ Erweiterung der Abwehrmechanismen
- □ Statistik für Nutzer

Zukunftsvisionen

- □ Repository auf Github
- □ Erweiterung der Abwehrmechanismen
- □ Statistik für Nutzer
- □ Effizienzsteigerung

Raum für Fragen