Hounterfeit
A virtual self-defending infrastructure with transparent relocation to honeypots

Mihai-Alexandru Bogatu

Coordinated by:

Adrian-Razvan Deaconescu

Catalin-Adrian Leordeanu

Whoami

- Education
  - University: ACS-UPB – BE, Master, PhD student
  - Certs: OSCP, MPT

- Penetration Tester 3+ years

- CTF Challenge Author 3+ years

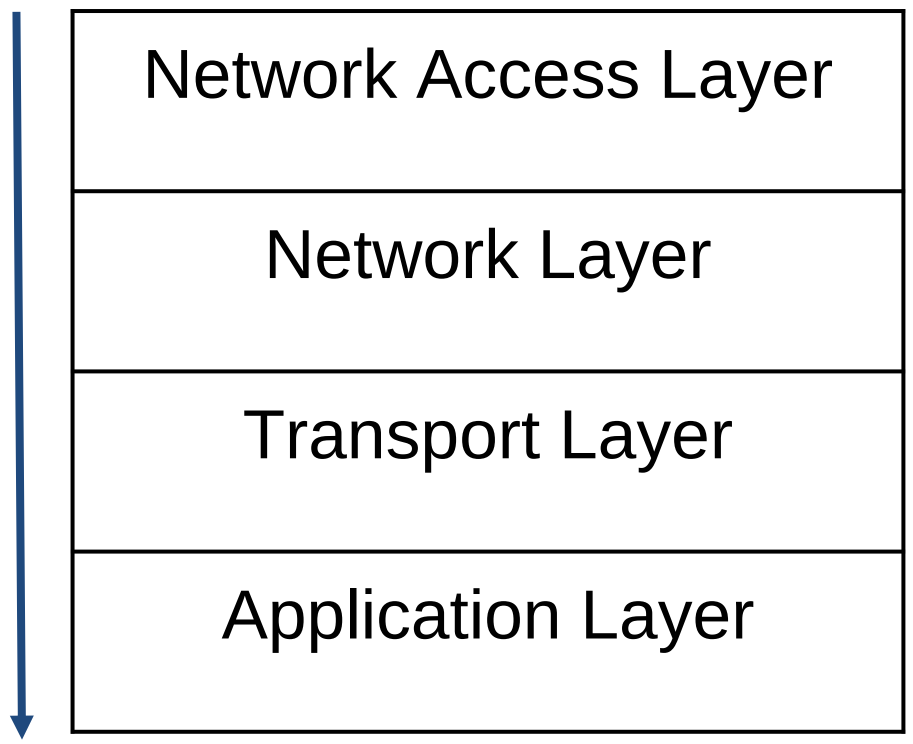
Problem

Advanced Persistent Threats

- Where/when to block the attack?
  - IDS/IPS
- How to keep up?
  - Rules
  - Behavior
  - ML
- Deceive? - Honeypots
  - Usually not representative

Firewalls & Honeypots

Firewalls
- Packet Filters
- Stateful Filters
- Next-Generation Firewalls



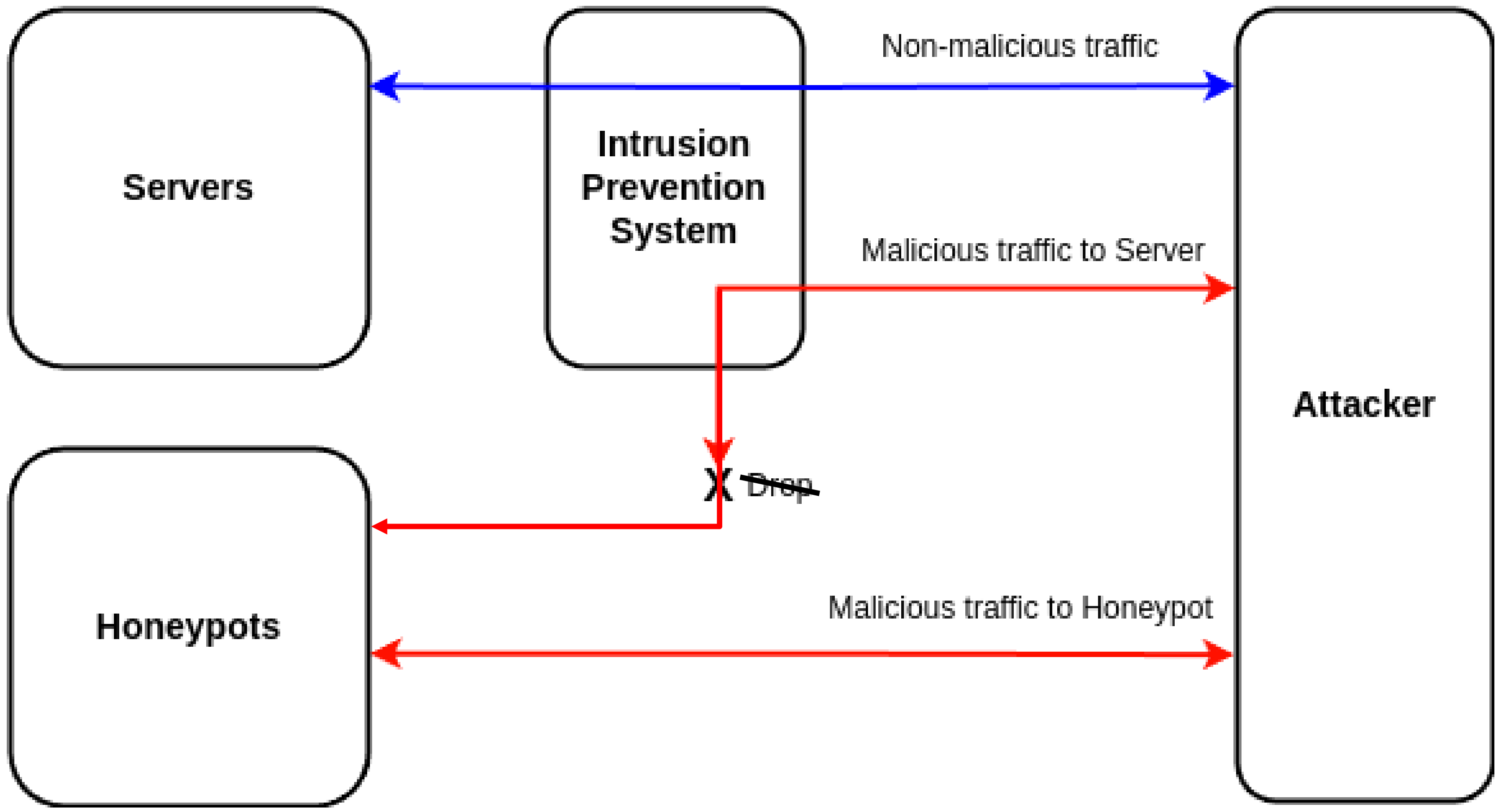
Honeypots
- Low-Interaction Honeypots
- High-Interaction Honeypots

Intrusion Prevention System (IPS)

Pros:
- Attacks are blocked before causing impact

Cons:
- Race between trial and error on obfuscating payloads and patching application

Solution:
- Migrate attacks to Honeypots
- Honeypots built from Server template

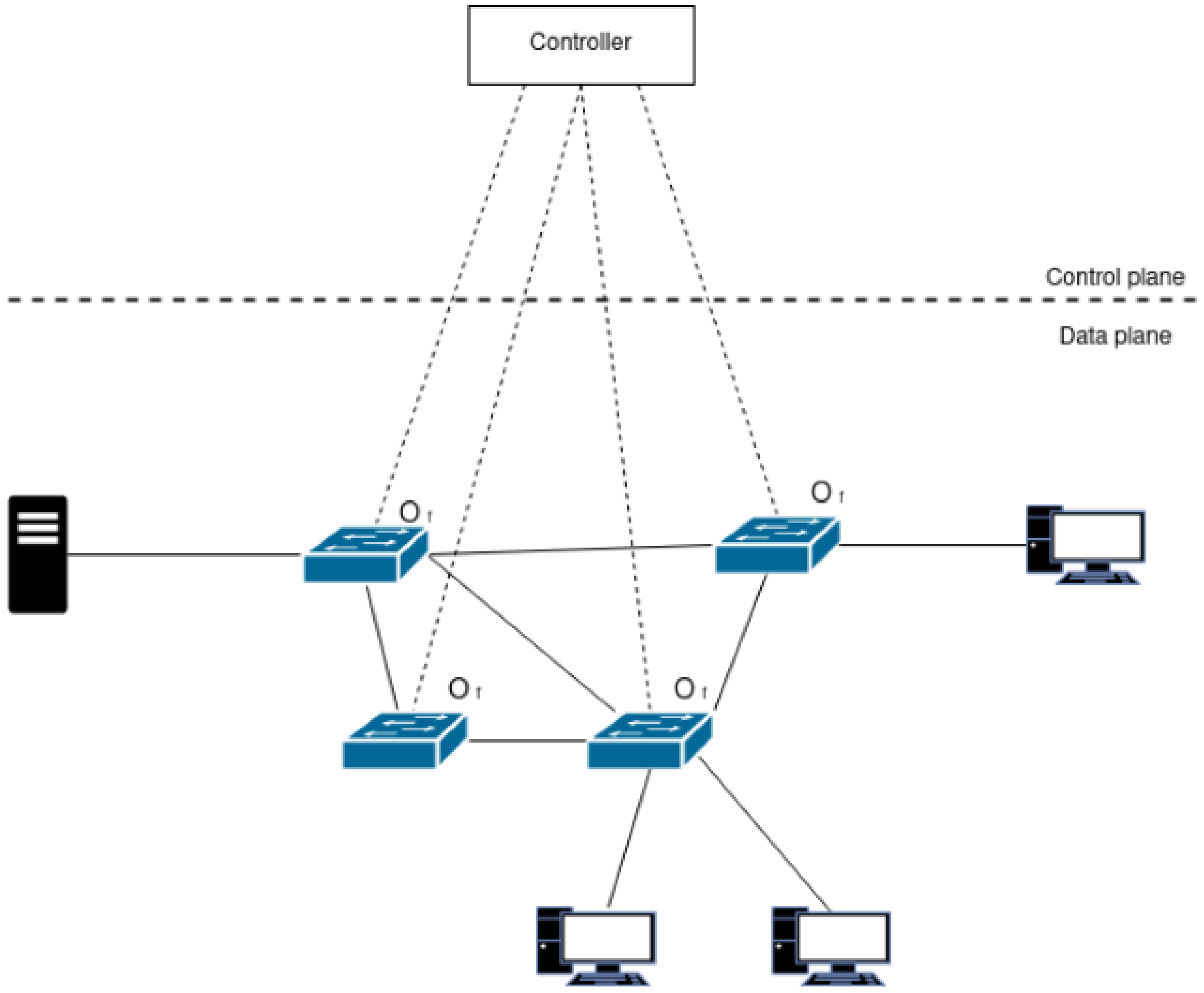


Software Defined Networking (SDN)

- Programmable network control

- Planes
  - Data
    - Switches
    - Servers/Applications
  - Control
    - SDN controller('s)

- Rules
  - Proactive
  - Reactive



State of the Art

Network level:

- OFSoftswitch
  - Advanced OpenFlow Switch for redirection
- Honeydoc
  - Controller level TCP-proxy

Process level:

- Linux Functions
  - TCP repair
- MfHoney
  - CRIU images modify sockets to LIH-HIH

Article	Mitigation Focus	SDN Controller	Deployment	Honeypot Type	Forwarding	Year
[6]	APT	No	Adaptive	N/A	No	2023
[7]	LIH/HIH + TCP Fingerprinting	No	Reactive	HIH	Transparent (CRIU - local)	2022
[8]	Detect Anomaly	Ryu	Proactive MTD	Not specified	No	2022
[9]	APT	Yes	Reactive at Pivoting	HIH	No	2022
[10]	Generic Decoy	ONOS	Reactive	Hybrid	No	2020
[11]	TCP Fingerprinting	Ryu	Proactive	HIH	Transparent (At Proxy)	2020
[12]	DDoS	ONOS	Reactive	HIH	Yes	2020
[13]	APT	Yes	Reactive	Container Replicas	Transparent (Container Clone)	2019
[14]	LIH/HIH + TCP Fingerprinting	Ryu	Reactive	Hybrid	Transparent (At Controller)	2019
[15]	Scans, DDoS	Ryu	Proactive MTD	MIH	No	2019
[16]	Integrity attacks, Zero-day	Yes	Proactive	VMs Replicas	Yes	2019
[17]	LIH/HIH Fingerprinting	Floodlight	Proactive	Hybrid	Yes	2019
[18]	LIH/HIH + TCP Fingerprinting	Ryu	Proactive	Hybrid	Transparent (At OpenFlow Switch)	2017
[19]	Generic Decoy	Yes	Proactive	Hybrid	No	2017
[20]	LIH/HIH Fingerprinting	POX	Proactive	Hybrid	Yes	2017
[21]	LIH/HIH Fingerprinting	Yes	Proactive	Hybrid	Yes	2016
[22]	Targeted Zero-day	Ryu	Reactive	VM Replica	Transparent (VM Clone)	2015

[6] S. Bagheri, H. Kermabon-Bobinnec, S. Majumdar, Y. Jarraya, L. Wang, and M. Pourzandi, "Warping the defence timeline: Non-disruptive proactive attack mitigation for kubernetes clusters," in *ICC 2023 - IEEE International Conference on Communications*, pp. 777–782, 2023.

[7] J. C. Acosta, "Locally-hosted fidelity-adaptive honeypots with connection-preserving capabilities," in *MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM)*, pp. 154–159, 2022.

[8] P. T. Duy, H. D. Hoang, N. H. Khoa, D. T. Thu Hien, and V.-H. Pham, "Fool your enemies: Enable cyber deception and moving target defense for intrusion detection in sdn," in *2022 21st International Symposium on Communications and Information Technologies (ISCIT)*, pp. 27–32, 2022.

[9] C. S. Bontas, I.-M. Stan, and R. Rughinis, "Honeypot generator using software defined networks and recursively defined topologies," in *2022 21st RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1–5, 2022.

[10] M. B. de Freitas, P. Quitério, L. Rosa, T. Cruz, and P. Simões, "Sdn-assisted containerized security and monitoring components," in *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, pp. 1–5, 2020.

[11] V. A. Cunha, D. Corujo, J. P. Barraca, and R. L. Aguiar, "Using linux tcp connection repair for mid-session endpoint handover: a security enhancement use-case," in *2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pp. 174–180, 2020.

[12] A. M. Zarca, J. B. Bernabe, A. Skarmeta, and J. M. Alcaraz Calero, "Virtual iot honeynets to mitigate cyberattacks in sdn/nfv-enabled iot networks," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1262–1277, 2020.

[13] A. Osman, P. Bruckner, H. Salah, F. H. P. Fitzek, T. Strufe, and M. Fischer, "Sandnet: Towards high quality of deception in container-based microservice architectures," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pp. 1–7, 2019.

[14] W. Fan, Z. Du, M. Smith-Creasey, and D. Fernández, "Honeydoc: An efficient honeypot architecture enabling all-round design," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 3, pp. 683-697, 2019.

[15] X. Luo, Q. Yan, M. Wang, and W. Huang, "Using mtd and sdn-based honeypots to defend ddos attacks in iot," in *2019 Computing, Communications and IoT Applications (ComComAp)*, pp. 392–395, 2019.

[16] G. Bernieri, M. Conti, and F. Pascucci, "Mimepot: a model-based honeypot for industrial control networks," in *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)*, pp. 433-438, 2019.

[17] H. Wang and B. Wu, "Sdn-based hybrid honeypot for attack capture," in *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, pp. 1602–1606, 2019.

[18] W. Fan and D. Fernandez, "A novel sdn based stealthy tcp connection handover mechanism for hybrid honeypot systems," in *2017 IEEE Conference on Network Softwarization (NetSoft)*, pp. 1–9, 2017.

[19] M. Valicek, G. Schramm, M. Pirker, and S. Schrittwieser, "Creation and integration of remote high interaction honeypots," in *2017 International Conference on Software Security and Assurance (ICSSA)*, pp. 50–55, 2017.

[20] S. Kyung, W. Han, N. Tiwari, V. H. Dixit, L. Srinivas, Z. Zhao, A. Doupé, and G.-J. Ahn, "Honeyproxy: Design and implementation of next-generation honeynet via sdn," in *2017 IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9, 2017.

[21] W. Han, Z. Zhao, A. Doupé, and G.-J. Ahn, "Honeymix: Toward sdn-based intelligent honeynet," in *Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*, SDN-NFV Security '16, (New York, NY, USA), p. 1–6, Association for Computing Machinery, 2016.

[22] A. Hirata, D. Miyamoto, M. Nakayama, and H. Esaki, "Intercept+: Sdn support for live migration-based honeypots," in *2015 4th International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)*, pp. 16-24, 2015.

Problem

Advanced Persistent Threats

- How to keep up?
  - Rules
  - Behavior
  - ML

✓ Where to block the attack?
  - Relocate instead of blocking

✓ Deceive? - Honeypots
  - TCP/IP level relocation to Honeypots
    - Application state?

State of the Art

- INTERCEPT+
  - VM-level
- Sandnet & Warp
  - Docker-level
- Hounterfeit
  - Process-level

Article	Mitigation Focus	SDN Controller	Deployment	Honeypot Type	Forwarding	Year
[6]	APT	No	Adaptive	N/A	No	2023
[7]	LIH/HIH + TCP Fingerprinting	No	Reactive	HIH	Transparent (CRIU - local)	2022
[8]	Detect Anomaly	Ryu	Proactive MTD	Not specified	No	2022
[9]	APT	Yes	Reactive at Pivoting	HIH	No	2022
[10]	Generic Decoy	ONOS	Reactive	Hybrid	No	2020
[11]	TCP Fingerprinting	Ryu	Proactive	HIH	Transparent (At Proxy)	2020
[12]	DDoS	ONOS	Reactive	HIH	Yes	2020
[13]	APT	Yes	Reactive	Container Replicas	Transparent (Container Clone)	2019
[14]	LIH/HIH + TCP Fingerprinting	Ryu	Reactive	Hybrid	Transparent (At Controller)	2019
[15]	Scans, DDoS	Ryu	Proactive MTD	MIH	No	2019
[16]	Integrity attacks, Zero-day	Yes	Proactive	VMs Replicas	Yes	2019
[17]	LIH/HIH Fingerprinting	Floodlight	Proactive	Hybrid	Yes	2019
[18]	LIH/HIH + TCP Fingerprinting	Ryu	Proactive	Hybrid	Transparent (At OpenFlow Switch)	2017
[19]	Generic Decoy	Yes	Proactive	Hybrid	No	2017
[20]	LIH/HIH Fingerprinting	POX	Proactive	Hybrid	Yes	2017
[21]	LIH/HIH Fingerprinting	Yes	Proactive	Hybrid	Yes	2016
[22]	Targeted Zero-day	Ryu	Reactive	VM Replica	Transparent (VM Clone)	2015

[6] S. Bagheri, H. Kermabon-Bobinnec, S. Majumdar, Y. Jarraya, L. Wang, and M. Pourzandi, "Warping the defence timeline: Non-disruptive proactive attack mitigation for kubernetes clusters," in *ICC 2023 - IEEE International Conference on Communications*, pp. 777–782, 2023.

[7] J. C. Acosta, "Locally-hosted fidelity-adaptive honeypots with connection-preserving capabilities," in *MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM)*, pp. 154–159, 2022.

[8] P. T. Duy, H. D. Hoang, N. H. Khoa, D. T. Thu Hien, and V.-H. Pham, "Fool your enemies: Enable cyber deception and moving target defense for intrusion detection in sdn," in *2022 21st International Symposium on Communications and Information Technologies (ISCIT)*, pp. 27–32, 2022.

[9] C. S. Bontas, I.-M. Stan, and R. Rughinis, "Honeypot generator using software defined networks and recursively defined topologies," in *2022 21st RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1–5, 2022.

[10] M. B. de Freitas, P. Quitério, L. Rosa, T. Cruz, and P. Simões, "Sdn-assisted containerized security and monitoring components," in *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, pp. 1–5, 2020.

[11] V. A. Cunha, D. Corujo, J. P. Barraca, and R. L. Aguiar, "Using linux tcp connection repair for mid-session endpoint handover: a security enhancement use-case," in *2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pp. 174–180, 2020.

[12] A. M. Zarca, J. B. Bernabe, A. Skarmeta, and J. M. Alcaraz Calero, "Virtual iot honeynets to mitigate cyberattacks in sdn/nfv-enabled iot networks," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1262–1277, 2020.

[13] A. Osman, P. Bruckner, H. Salah, F. H. P. Fitzek, T. Strufe, and M. Fischer, "Sandnet: Towards high quality of deception in container-based microservice architectures," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pp. 1–7, 2019.

[14] W. Fan, Z. Du, M. Smith-Creasey, and D. Fernández, "Honeydoc: An efficient honeypot architecture enabling all-round design," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 3, pp. 683-697, 2019.

[15] X. Luo, Q. Yan, M. Wang, and W. Huang, "Using mtd and sdn-based honeypots to defend ddos attacks in iot," in *2019 Computing, Communications and IoT Applications (ComComAp)*, pp. 392–395, 2019.

[16] G. Bernieri, M. Conti, and F. Pascucci, "Mimepot: a model-based honeypot for industrial control networks," in *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)*, pp. 433-438, 2019.

[17] H. Wang and B. Wu, "Sdn-based hybrid honeypot for attack capture," in *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, pp. 1602–1606, 2019.

[18] W. Fan and D. Fernandez, "A novel sdn based stealthy tcp connection handover mechanism for hybrid honeypot systems," in *2017 IEEE Conference on Network Softwarization (NetSoft)*, pp. 1–9, 2017.

[19] M. Valicek, G. Schramm, M. Pirker, and S. Schrittwieser, "Creation and integration of remote high interaction honeypots," in *2017 International Conference on Software Security and Assurance (ICSSA)*, pp. 50–55, 2017.

[20] S. Kyung, W. Han, N. Tiwari, V. H. Dixit, L. Srinivas, Z. Zhao, A. Doupé, and G.-J. Ahn, "Honeyproxy: Design and implementation of next-generation honeynet via sdn," in *2017 IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9, 2017.

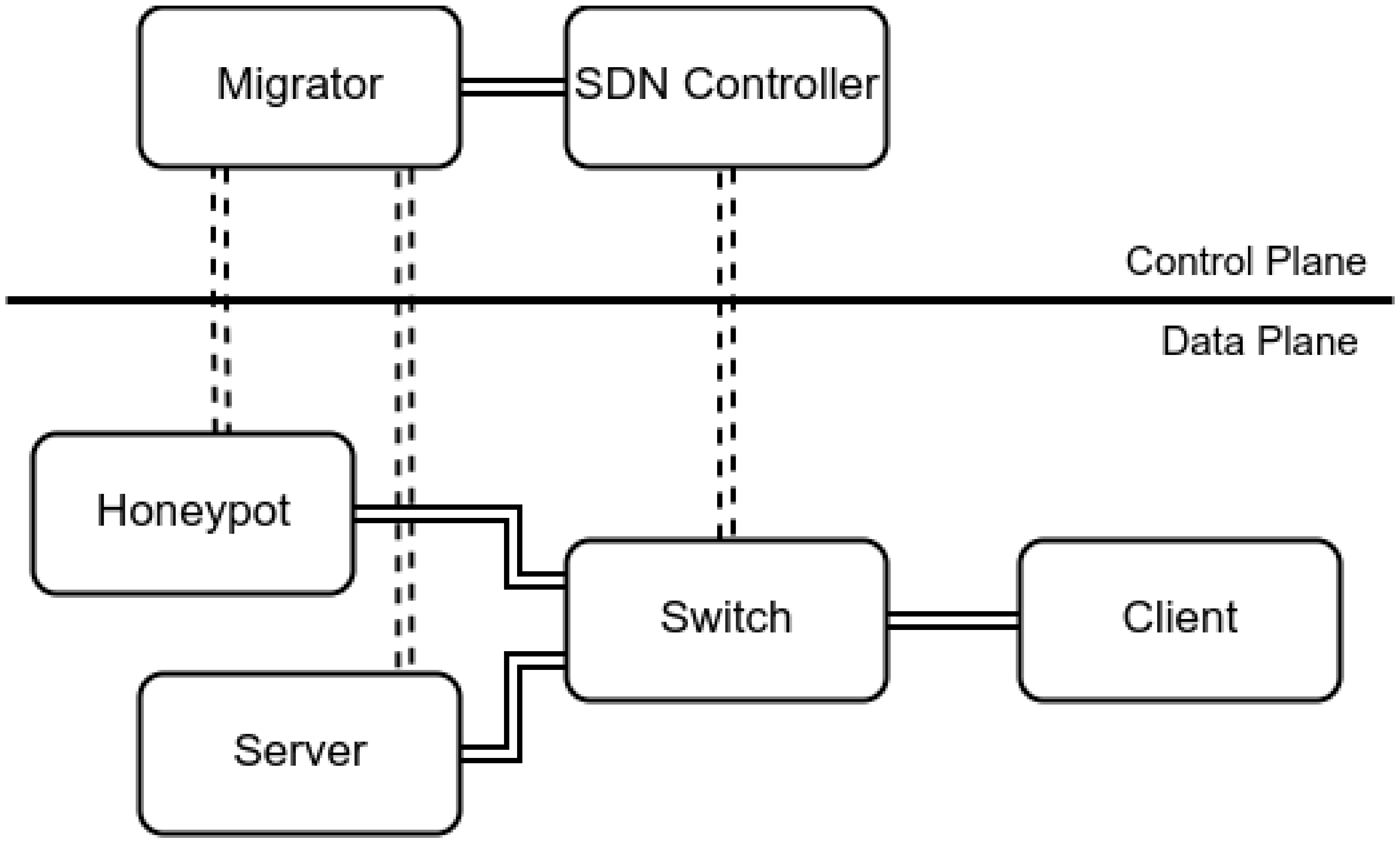
[21] W. Han, Z. Zhao, A. Doupé, and G.-J. Ahn, "Honeymix: Toward sdn-based intelligent honeynet," in *Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*, SDN-NFV Security '16, (New York, NY, USA), p. 1–6, Association for Computing Machinery, 2016.

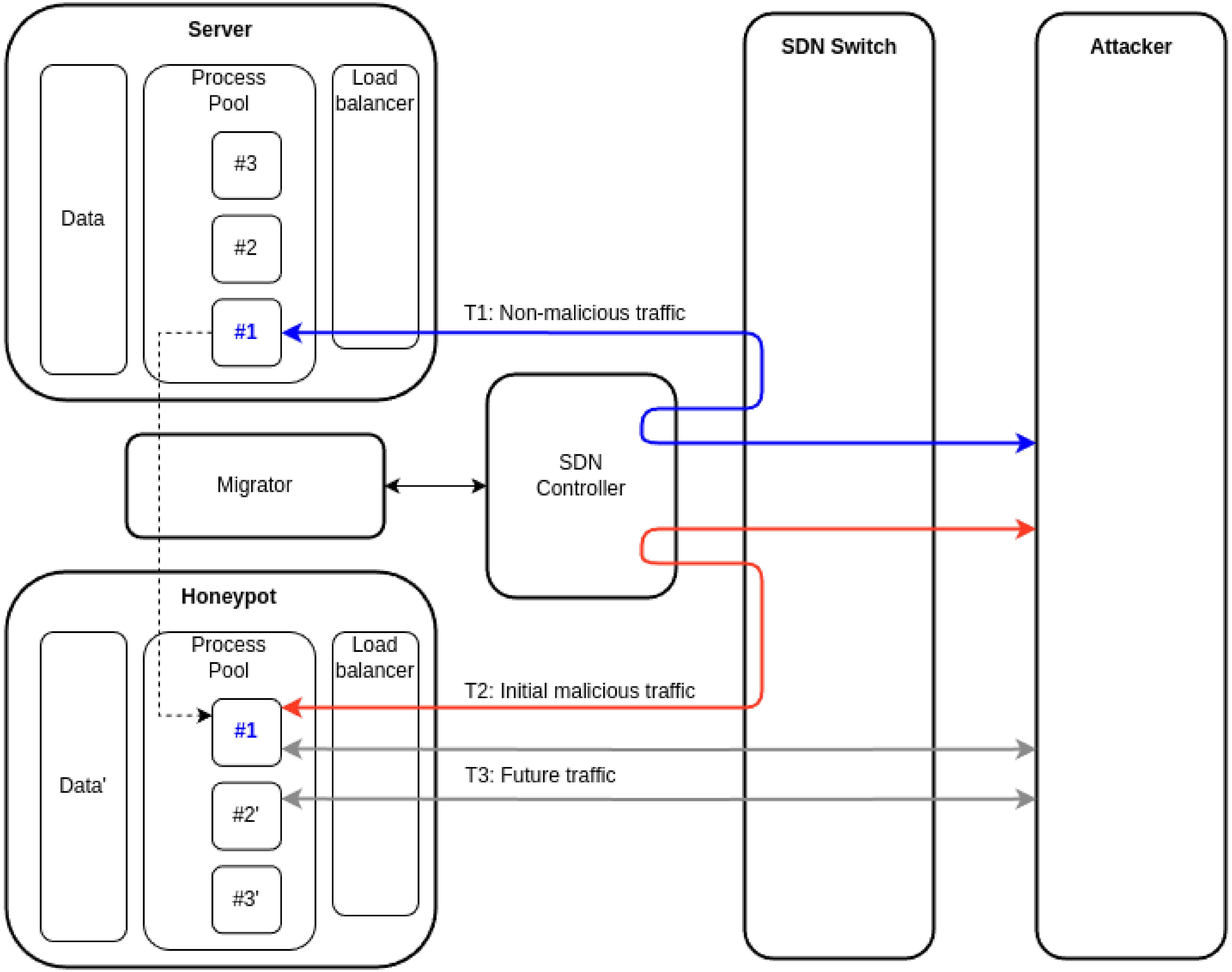
[22] A. Hirata, D. Miyamoto, M. Nakayama, and H. Esaki, "Intercept+: Sdn support for live migration-based honeypots," in *2015 4th International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)*, pp. 16-24, 2015.

Checkpoint/Restore in Userspace

"It can freeze a running container (or an individual application) and checkpoint its state to disk. The data saved can be used to restore the application and run it exactly as it was during the time of the freeze..." [CRIU.org Wiki]

Infrastructure

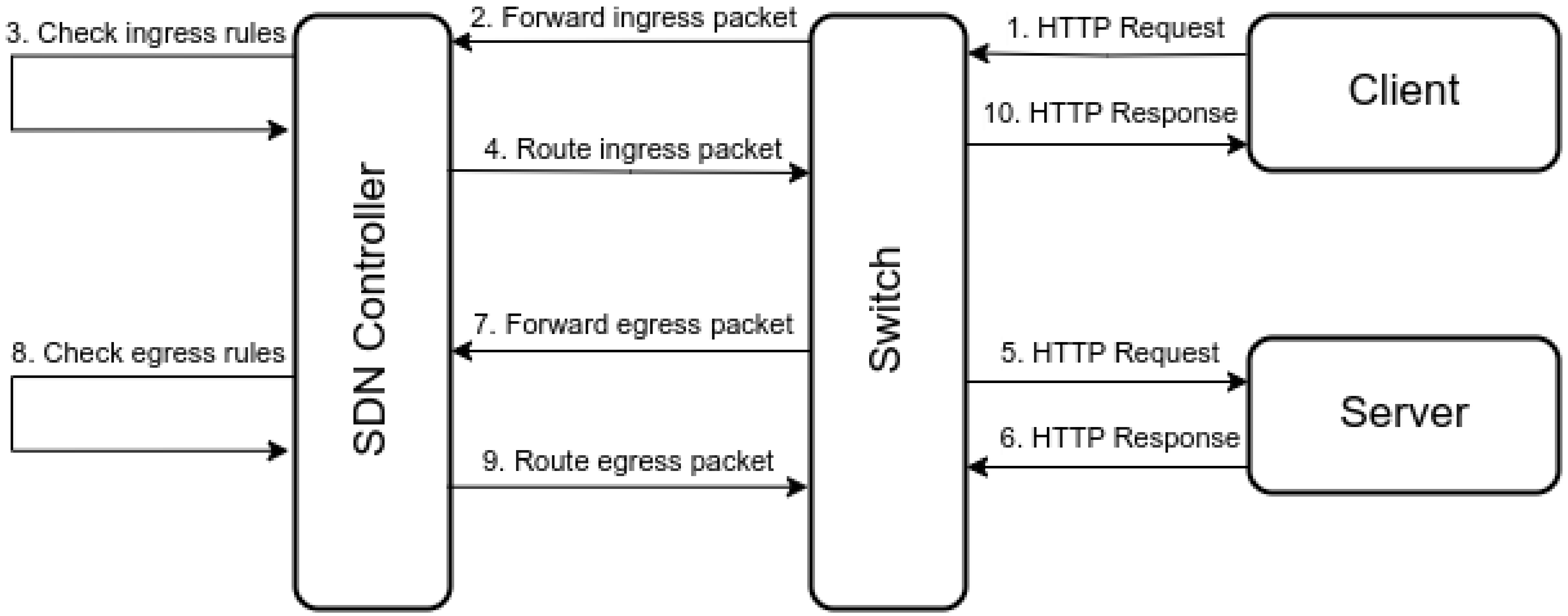



Server
Data
Process Pool
#3
#2
#1
Load balancer
T1: Non-malicious traffic
SDN Switch
Attacker
Migrator
SDN Controller
Honeypot
Data'
Process Pool
#1
#2'
#3'
Load balancer
T2: Initial malicious traffic
T3: Future traffic

Communication Flow

Detect:

- Ingress for payloads
  => migrate*
- Egress for sensitive data
  => drop
  => redirect



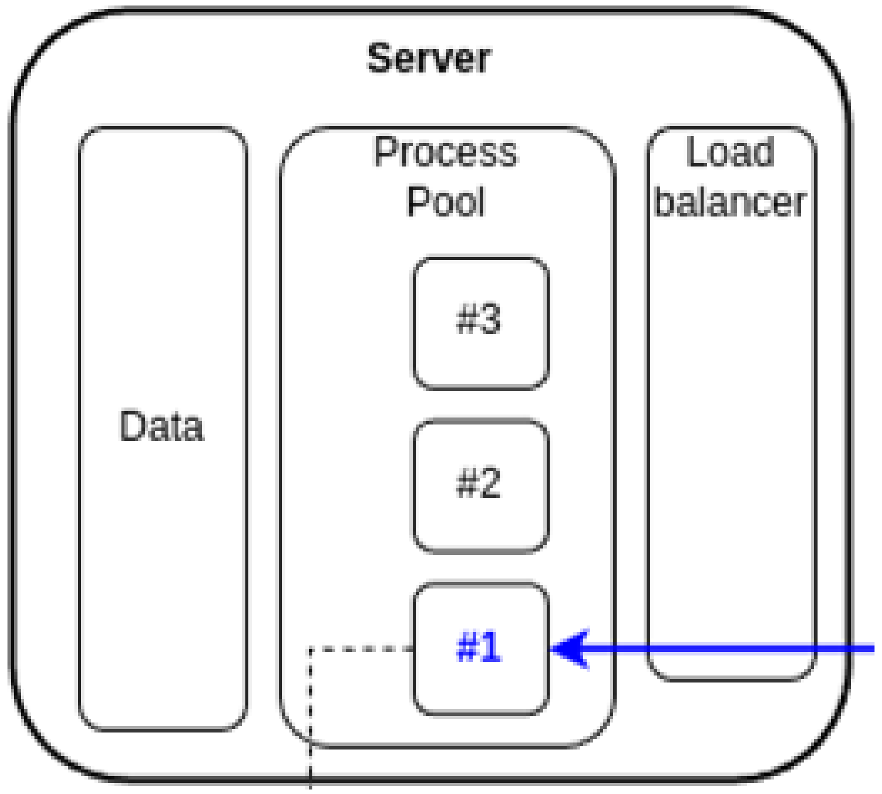
Sockets

TCP session - unique 4-tuple:

- Source IP + Port
- Destination IP + Port

Server side:

- Lifecycle: create,*bind*,listen,accept,..
- Listening address blocks
  - Bypass: socket option ***SO_REUSEPORT*** (Linux +3.9)
    - OS responsible for load-balancing



Sockets

What if program does not support ***SO_REUSEPORT*** ?

- Binary option: ***LD_PRELOAD***
  - Grab socket call
  - Add socket option

```c
typedef int (*socket_t)(int, int, int);

int socket(int domain, int type, int protocol)
{
    socket_t original_socket = (socket_t)dlsym(RTLD_NEXT, "socket");
    int sockfd = original_socket(domain, type, protocol);

    if (sockfd < 0)
    {
        return sockfd;
    }

    int opt = 1;
    setsockopt(sockfd, SOL_SOCKET, SO_REUSEPORT, &opt, sizeof(opt));

    return sockfd;
}
// gcc - shared - fPIC - o reuseport_wrapper.so so_reuseport_ld.c - ldl
```

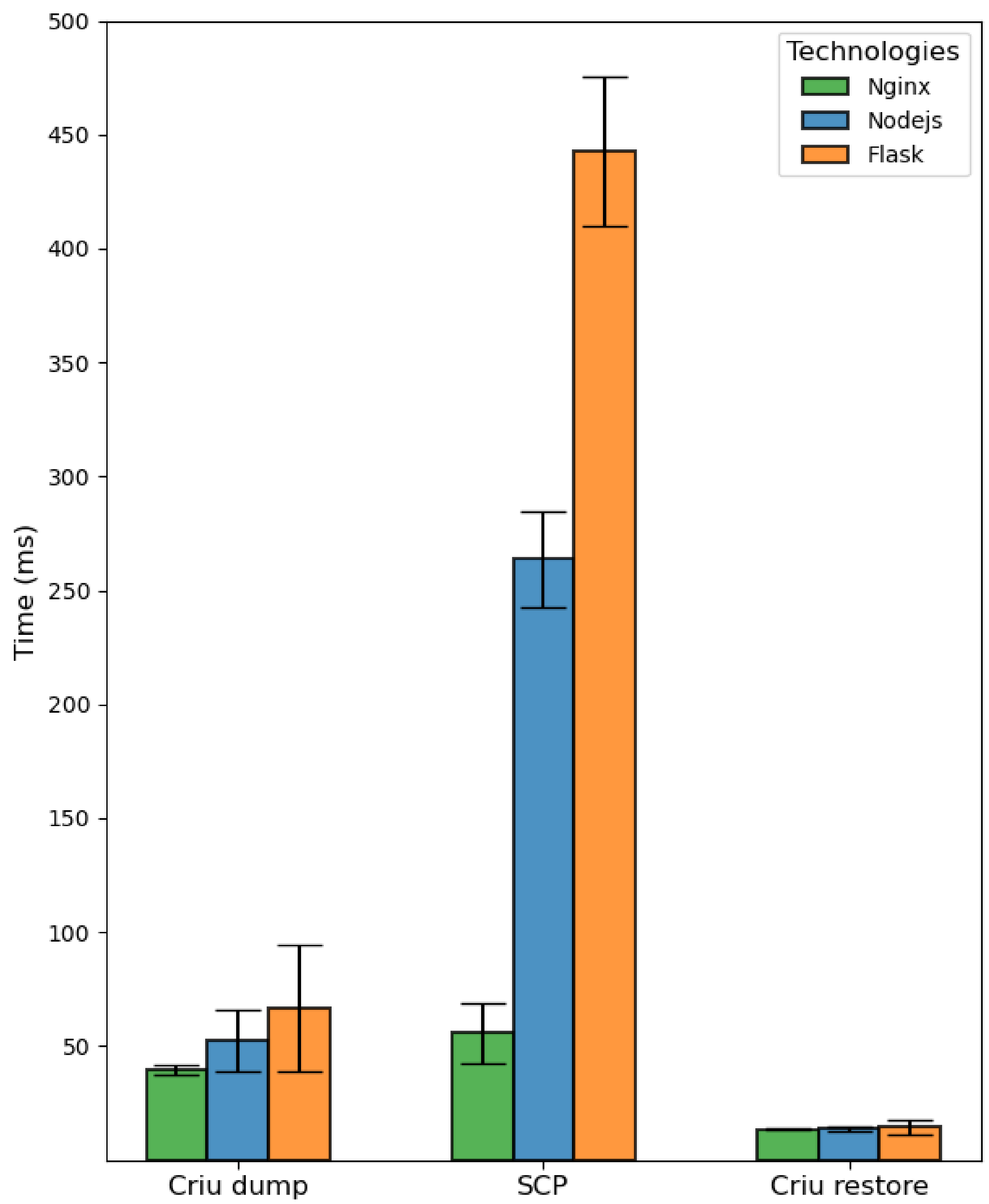
Metrics

Under test (HTTP):

- Nginx
- Nodejs
- Flask

Service	Criu dump	SCP transfer	Criu Restore	Total
Nginx	39.57 | 2.16(σ)	55.82 | 13.19(σ)	13.47 | 0.22(σ)	108.87 | 13.39(σ)
Node	52.40 | 13.62(σ)	263.72 | 20.92(σ)	13.63 | 0.93(σ)	329.76 | 23.01(σ)
Flask	66.70 | 27.53(σ)	442.40 | 32.78(σ)	14.40 | 3.31(σ)	523.50 | 38.65(σ)

Table 1: Mean and Standard Deviation of step per technology, measured in ms.

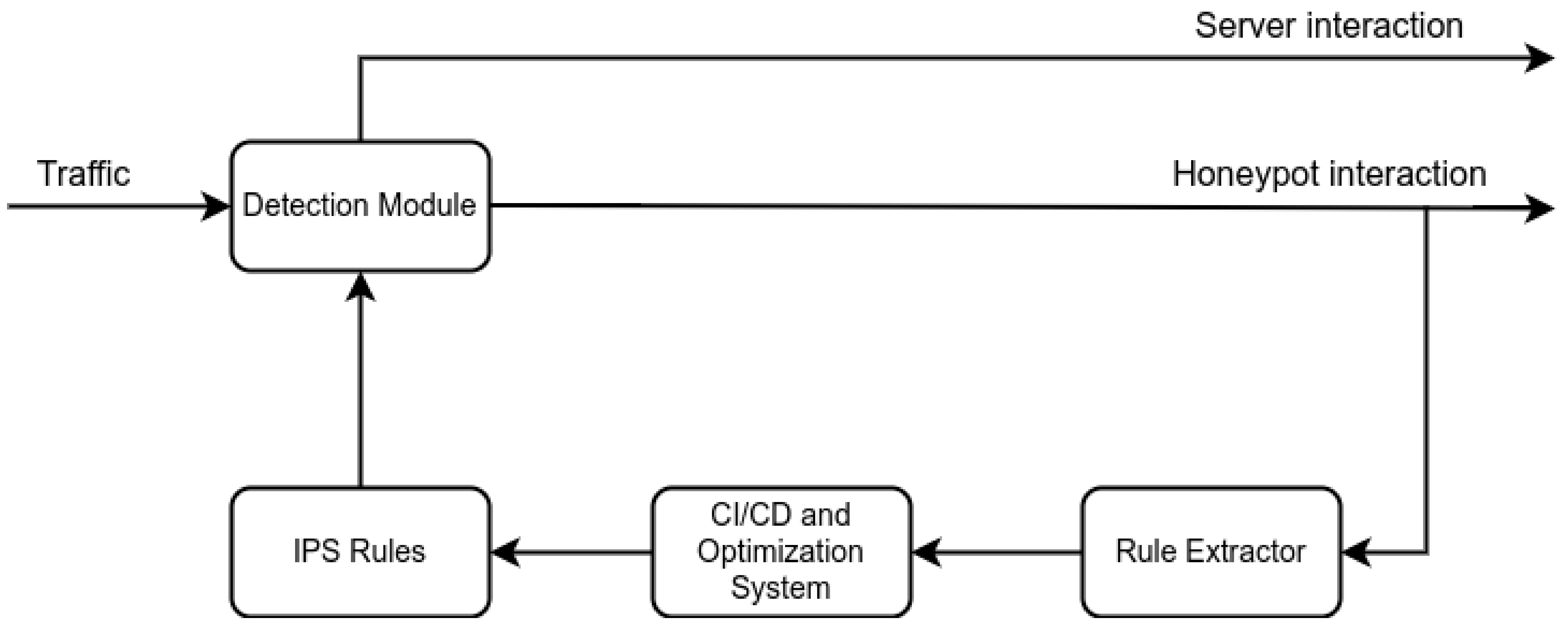


```
root@ubuntu-focal:/home/vagrant#
```

Limitations

- Encrypted traffic
- Multi-process migration
- NAT clients backfire
- Truncated packets
- Client-Side attacks

Next steps


Server interaction
Traffic
Detection Module
Honeypot interaction
IPS Rules
CI/CD and Optimization System
Rule Extractor

Conclusions

- Live attack redirection
- Transparent relocation
- Within standard network timeouts
- Scalable architecture
- Customized IDPS rules:
  Free payloads from attacks without impact!*

Thank you!