3

Can You Spot the Trap? Honeypot Detection in the Face of Evolving Evasion Tactics (SoK)

Mathis DURAND [1] IMT Atlantique, IRISA, Cyber CNI
Alexandre DEY [2] Airbus CyberSecurity, Cyber CNI
Yvon KERMARREC [1] IMT Atlantique, Lab-STICC
Marc-Oliver PAHL [1] IMT Atlantique, IRISA, Cyber CNI

[1] {firstname}.{name}@imt-atlantique.fr
[2] alexandre.dey@airbus.com

presenter: Mathis DURAND

Introduction

Definition and missions

[Crowdstrike2025honeypot]

“A **honeypot** is a cybersecurity mechanism that uses a manufactured attack target to **lure cybercriminals away** from legitimate targets. They also **gather intelligence** about the identity, methods and motivations of adversaries.”

Missions of honeypot:

→Detect suspicious actions
→Decoy attackers
→Gather Cyber Threat Intelligence

[Crowdstrike2025honeypot] https://www.crowdstrike.com/en-au/cybersecurity-101/exposure-management/honeypots/

Introduction

Structure

Why detecting honeypots?

Why a new SoK?

How to describe detection techniques?

What are the trends?

How to mitigate?

Introduction

Structure

Introduction

Motivation

Taxonomy

Analysis

Mitigation

3

Introduction

Motivation

Honeypot detection taxonomy

Detection techniques analysis

Mitigation

Motivation

ARP-based detection [boulaiche2008honeyd]

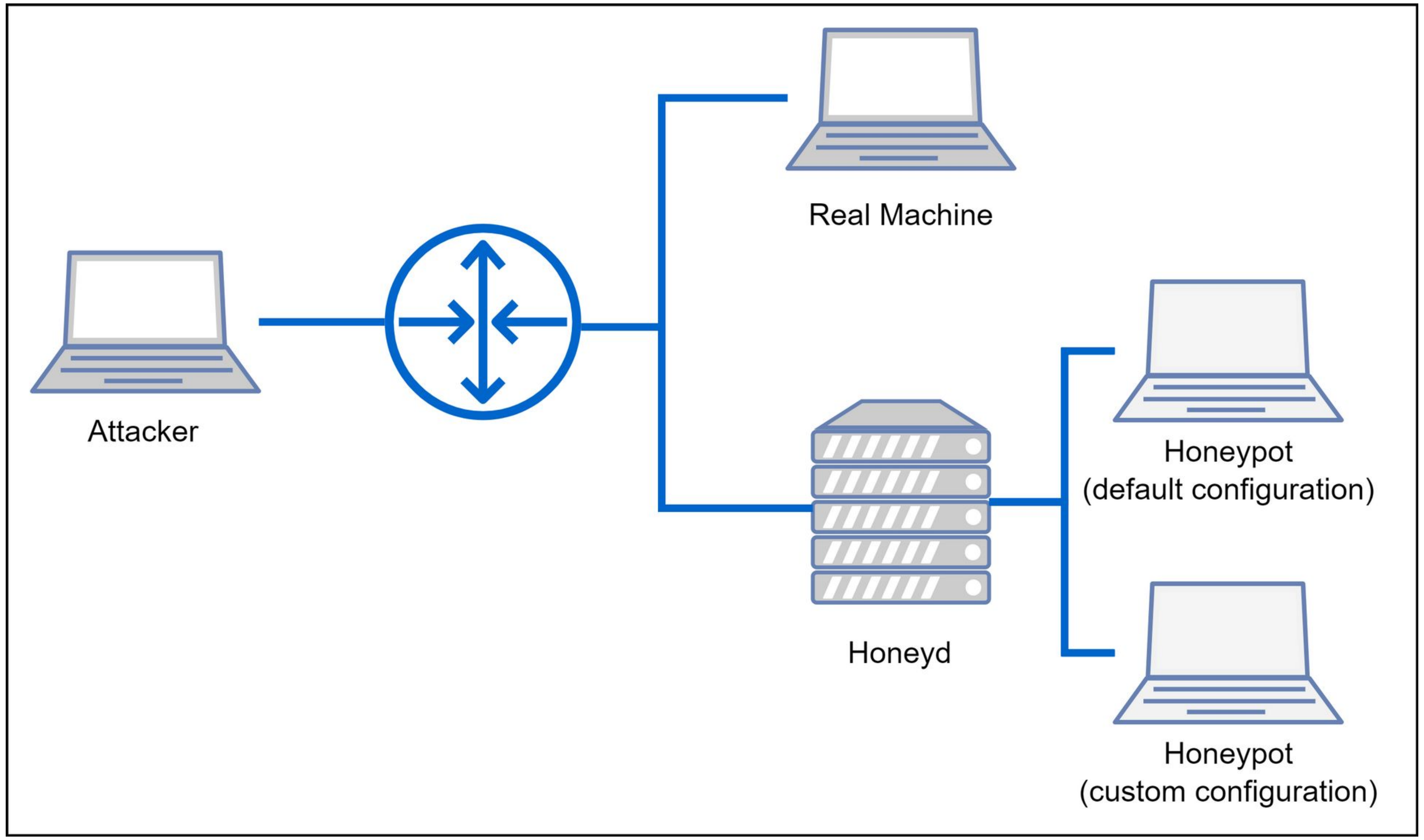


Fig.1: Architecture of a network using Honeyd

Honeyd-based honeypot
ARP analysis

[boulaiche2008honeyd] A. Boulaiche, K. Adi, Honeyd detection via abnormal behaviors generated by the arpd daemon., in: SECRYPT, 2008, pp. 65–71

Motivation

ARP-based detection [boulaiche2008honeyd]

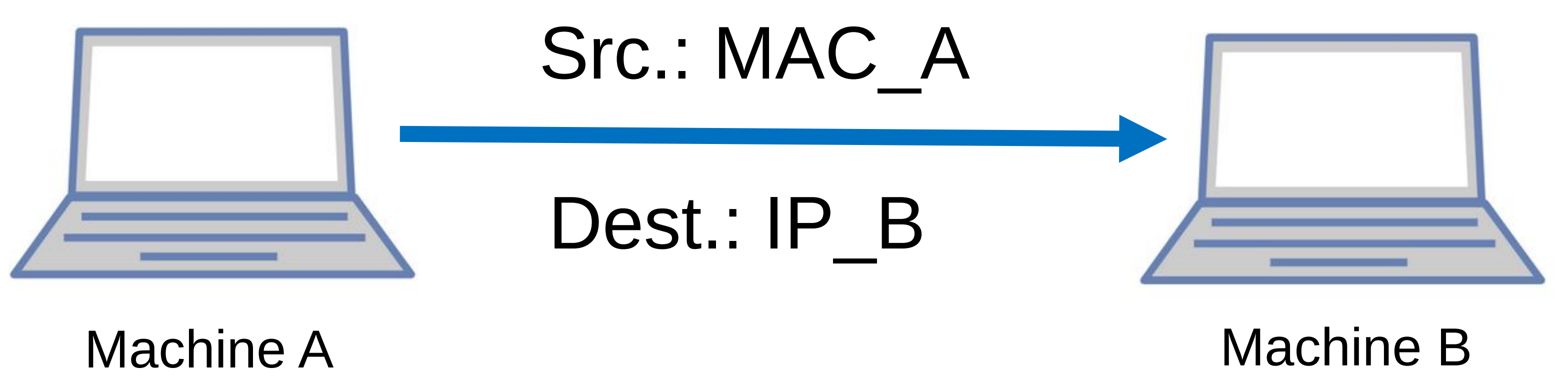


Fig.2a: ARP request

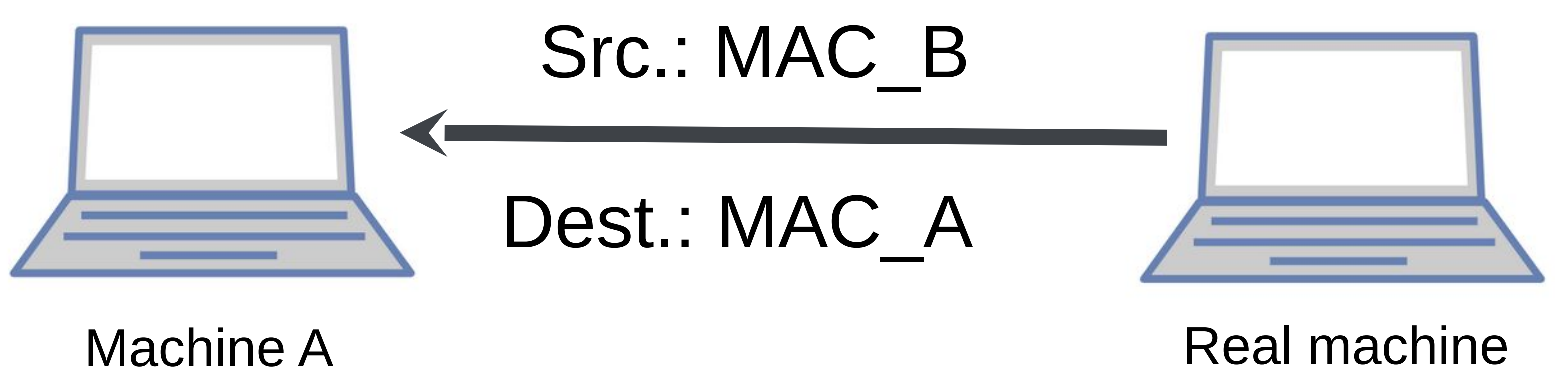


Fig.2b: ARP real machine response

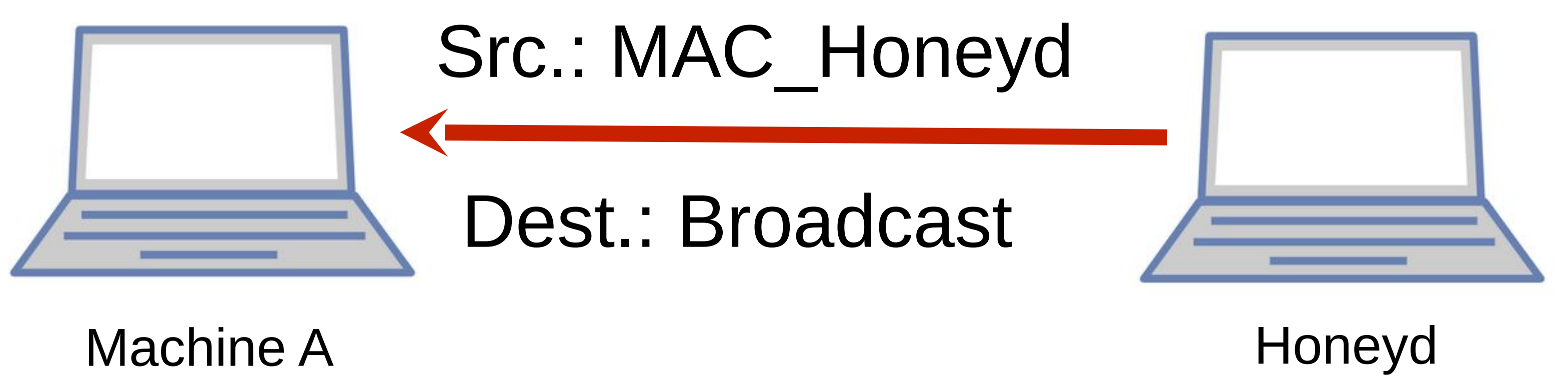


Fig.2c: ARP honeyd response

[boulaiche2008honeyd] A. Boulaiche, K. Adi, Honeyd detection via abnormal behaviors generated by the arpd daemon., in: SECRYPT, 2008, pp. 65–71

Motivation

Related work

			Strategy		Type		Origin	
Reference	Year	Taxonomy	Evasion	Detection	Fingerprint	Behavior	Lab	Attack
[chen2008towards]	2008	◐	●		●	●		●
[lauren2017survey]	2017	◐		●	●		●	
[afianian2019survey]	2019	◐	●				●	●
]		◐		●	●		●	
Our SoK	2025	●	●	●	●	●	●	●

[chen2008towards] X. Chen, J. Andersen, Z. M. Mao, M. Bailey, J. Nazario, Towards an understanding of anti-virtualization and anti-debugging behavior in modern malware, in: 2008 IEEE international conference on dependable systems and networks with FTCS and DCC (DSN), IEEE, 2008, pp.177–186.
[lauren2017survey] S. Laurén, V. Leppänen, S. Rauti, J. Uitto, A survey on anti-honeypot and anti-introspection methods, Recent Advances in Information Systems and Technologies 2 (2017) 11–13.
[afianian2019survey] A. Afianian, S. Niksefat, B. Sadeghiyan, D. Baptiste, Malware dynamic analysis evasion techniques: A survey, ACM Computing Surveys (CSUR) 52 (2019) 1–28.
[tay2023taxonomy] V. Tay, X. Li, D. Mashima, B. Ng, P. Cao, Z. Kalbarczyk, R. K. Iyer, Taxonomy of fingerprinting techniques for evaluation of smart grid honeypot realism, in: 2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), IEEE, 2023, pp. 1–7.

3

Introduction

Motivation

Honeypot detection taxonomy

Detection techniques analysis

Mitigation

CYBER CNI.FR SOTERN AIRBUS

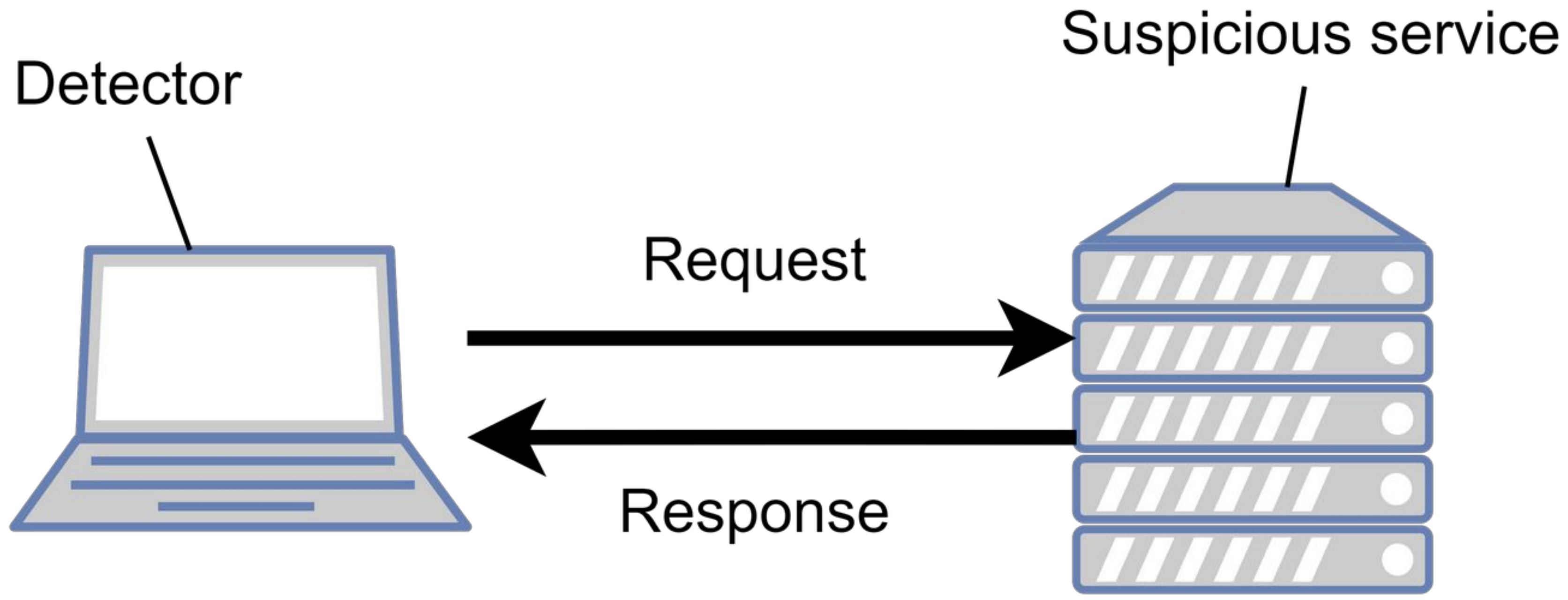
Honeypot detection taxonomy

Detection taxonomy – Vectors

Vector [WIP]	Example
Code	Default configuration, errors
Resource Level	Virtualization
Scenario	Human activity, difficulty of compromission
Purpose	Tools for CTI collection, decoy
Allowed Actions	Strange security configuration
Physical Integration	Sensor reponses

Honeypot detection taxonomy

Detection taxonomy – Detection type



Behavior	Response is suspicious, maybe not a honeypot
Fingerprint	Response could be legitimate, but I know a honeypot working like this

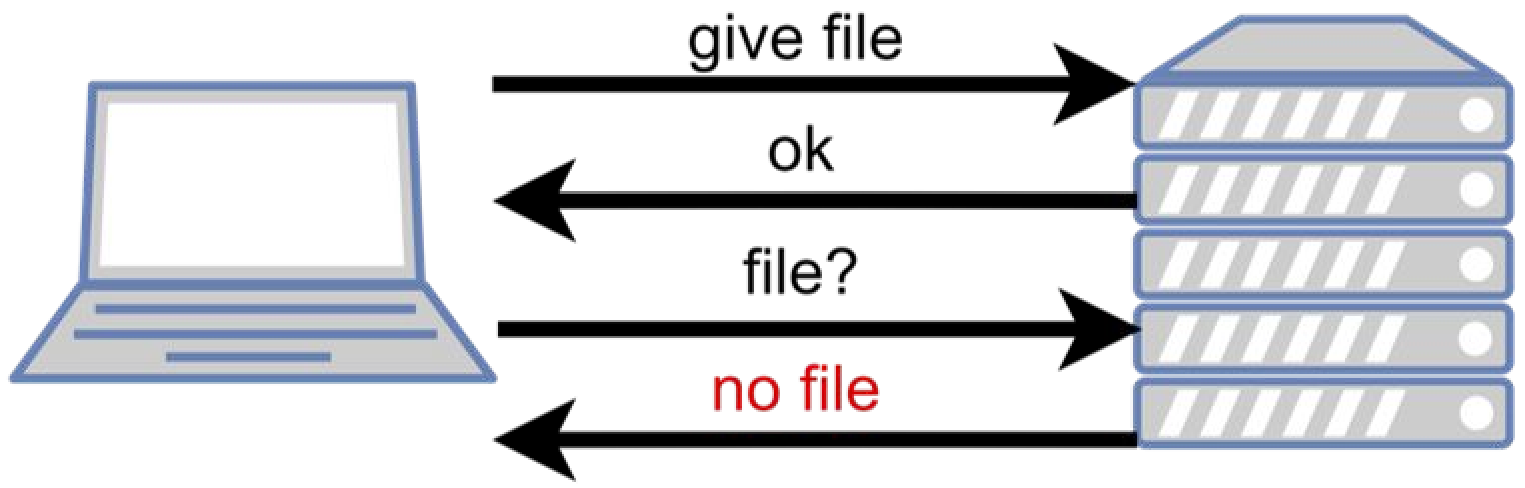


Fig.2a: *Behavior*-based detection use case

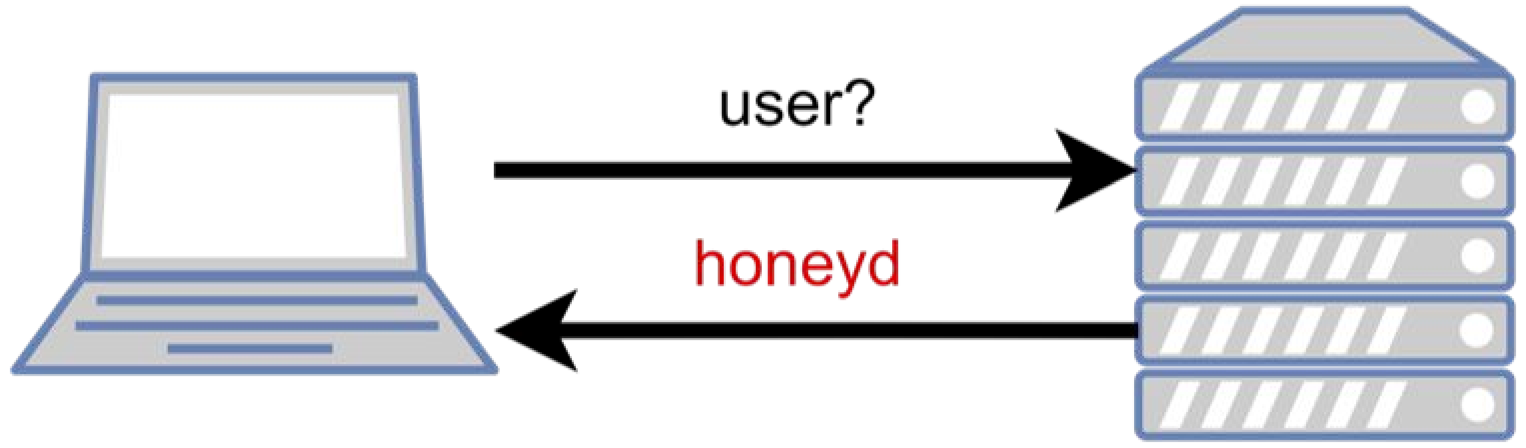


Fig.2b: *Fingerprint*-based detection use case

Honeypot detection taxonomy

Detection taxonomy – Data source

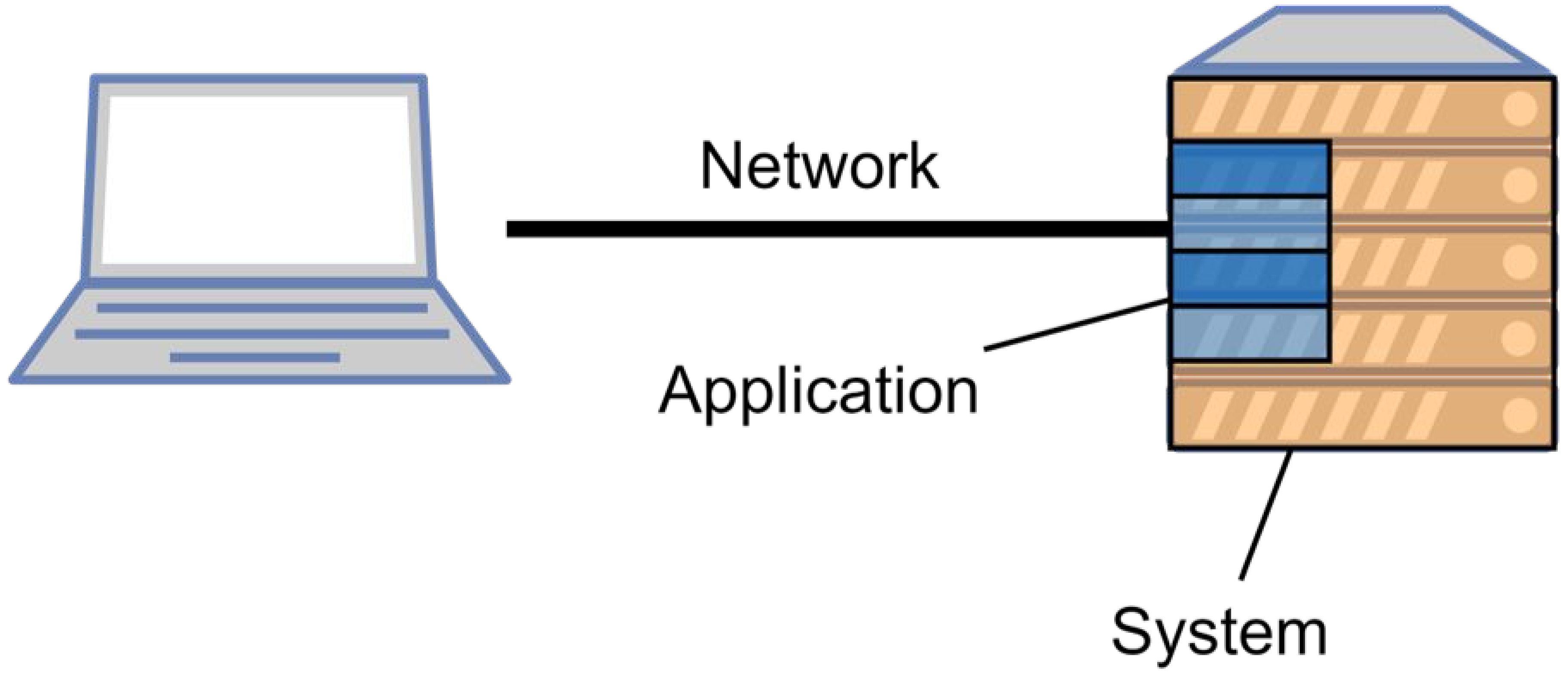


Fig.3: Data source of detection technique

Ref	Technique	Data source
[boulaiche2008honeyd]	Analyse ARP packets	Network
[chen2023honeypot]	Provoke errors	Application
[zhu2024honeyjudge]	Read memory	System

[boulaiche2008honeyd] A. Boulaiche, K. Adi, Honeyd detection via abnormal behaviors generated by the arpd daemon., in: SECRYPT, 2008, pp. 65–71
[chen2023honeypot] X. Chen, B. Lu, R. Sun, M. Jiang, Honeypot detection method based on anomalous requests response differences, in: Proceedings of the 2023 6th International Conference on Electronics, Communications and Control Engineering, 2023, pp. 109–117.
[zhu2024honeyjudge] H. Zhu, M. Liu, B. Chen, X. Che, P. Cheng, R. Deng, Honeyjudge: A plc honeypot identification framework based on device memory testing, IEEE Transactions on Information Forensics and Security (2024)

Honeypot detection taxonomy

Detection taxonomy – Location

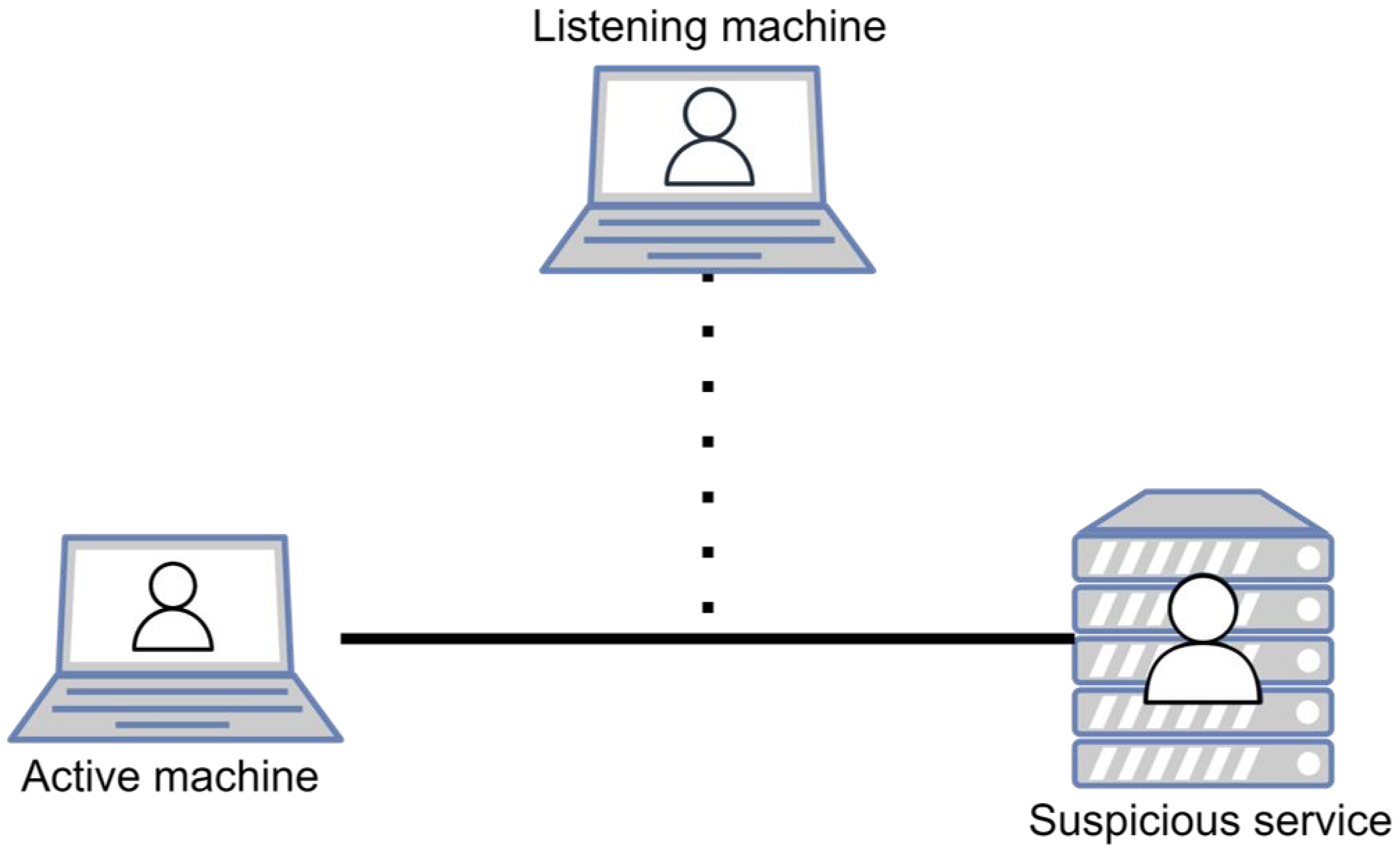


Fig.4: Location of detection technique

Ref	Technique	Location
[boulaiche2008honeyd]	Analyse ARP packets	Active machine
[surnin2019probabilistic]	Analyse shell responses	Service
[wenda2011honeypot]	Fingerprint Network	Listening machine

[boulaiche2008honeyd] A. Boulaiche, K. Adi, Honeyd detection via abnormal behaviors generated by the arpd daemon., in: SECRYPT, 2008, pp. 65–71
[surnin2019probabilistic] O. Surnin, F. Hussain, R. Hussain, S. Ostrovskaya, A. Polovinkin, J. Lee, X. Fernando, Probabilistic estimation of honeypot detection in internet of things environment, in: 2019 International Conference on Computing, Networking and Communications (ICNC), IEEE, 2019, pp. 191–196.
[wenda2011honeypot] D. Wenda, D. Ning, A honeypot detection method based on characteristic analysis and environment detection, in: 2011 International Conference in Electrics, Communication and Automatic Control Proceedings, Springer, 2011, pp. 201–206.

3

Introduction
Motivation
Honeypot detection taxonomy
Detection techniques analysis
Mitigation

CYBER CNI.FR SOTERN AIRBUS

Honeypot Detection in the Literature

Detection by Memory Testing [zhu2024honeyjudge]

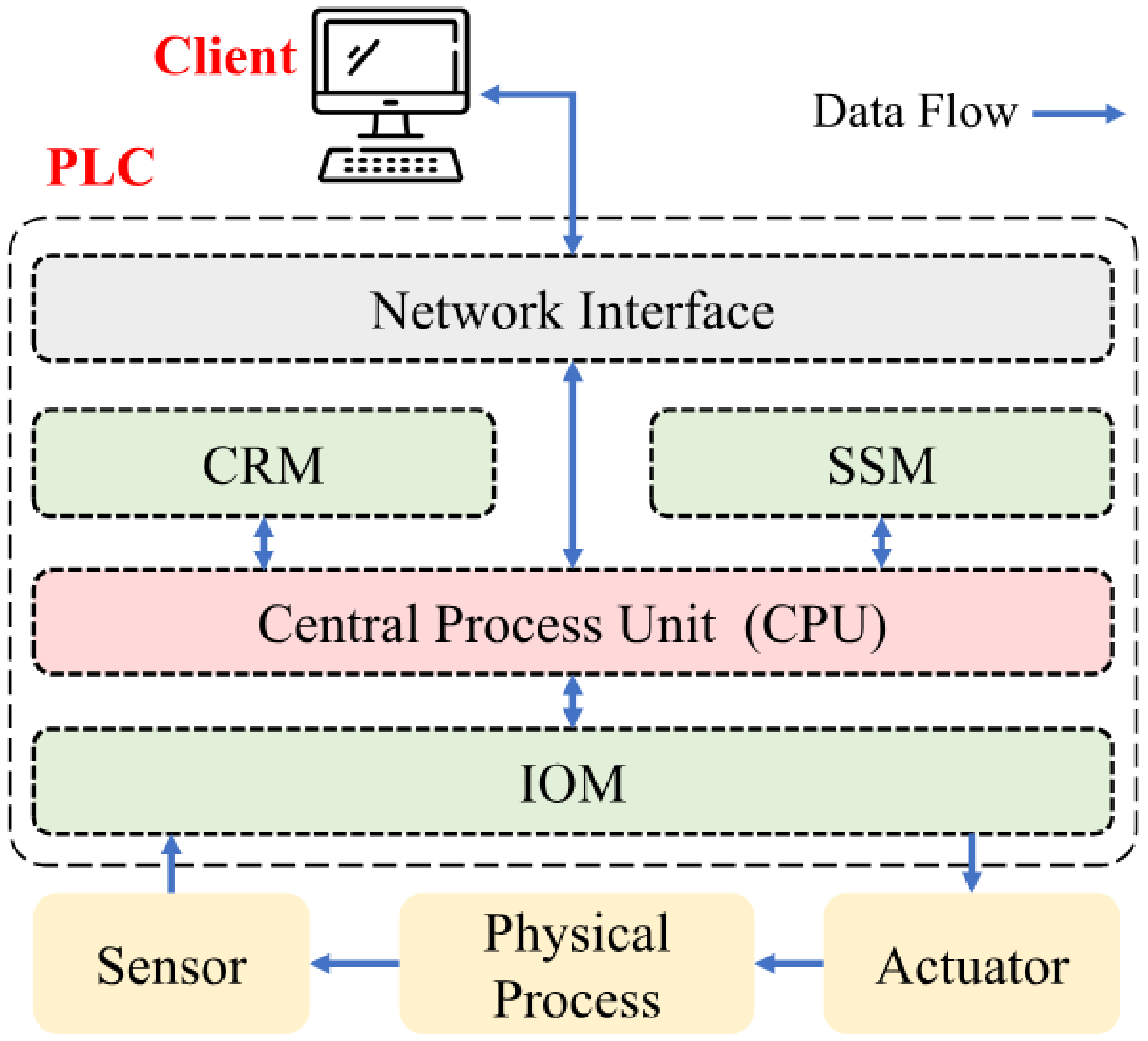


Fig.5: The memory architecture and connection within the PLC

PLC memory
- System State Memory
- Control Related Memory
- Input-Output Memory

PLC Honeypot
- Semantic conflicts
- Wrong variables
- Less Noise in I/O

[zhu2024honeyjudge] H. Zhu, M. Liu, B. Chen, X. Che, P. Cheng, R. Deng, Honeyjudge: A plc honeypot identification framework based on device memory testing, IEEE Transactions on Information Forensics and Security (2024)

Honeypot Detection in the Literature

Detection by Memory Testing [zhu2024honeyjudge]

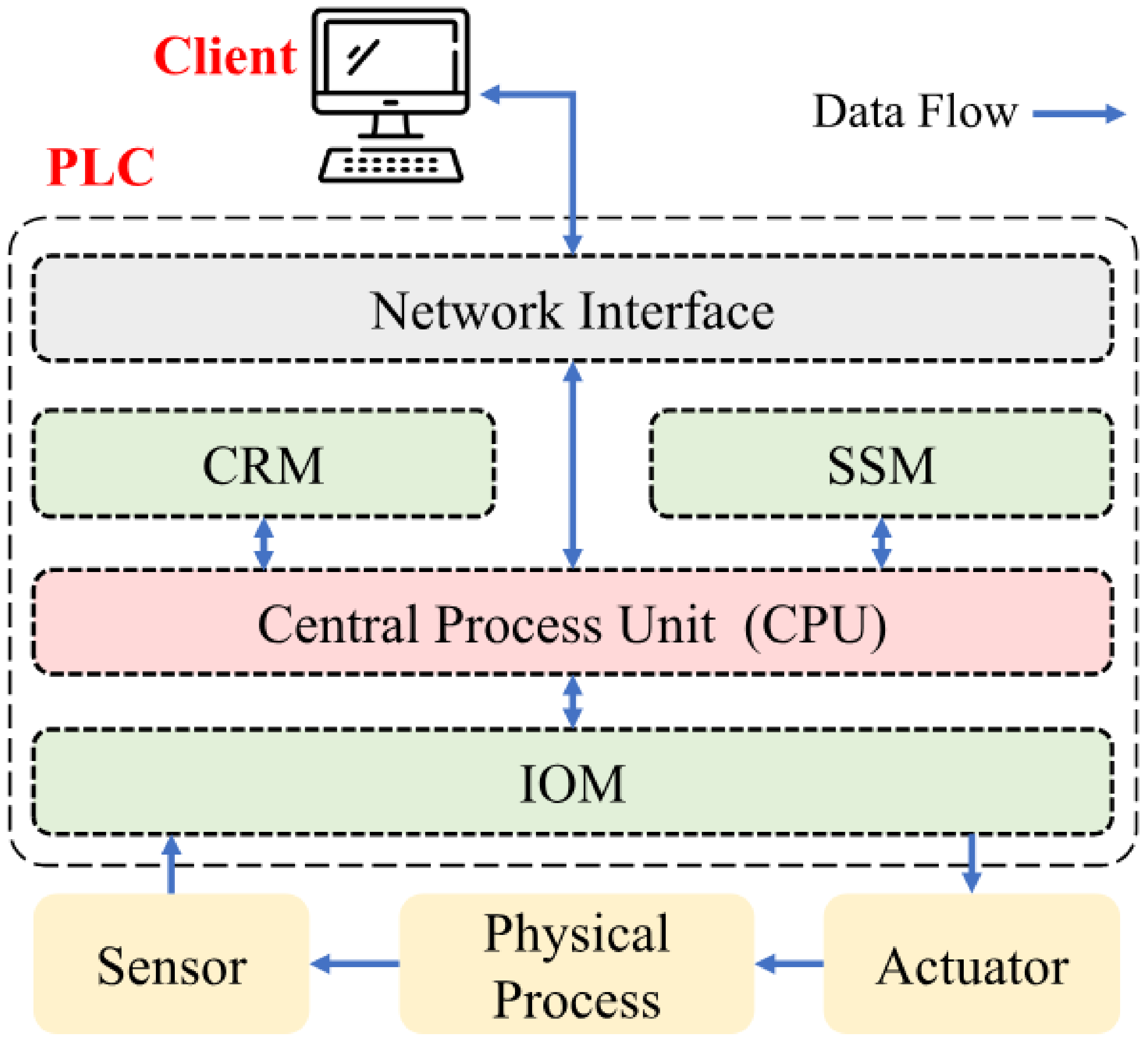


Fig.5: The memory architecture and connection within the PLC

[zhu2024honeyjudge]
- Detection vector: Resource Level
- Detection type: Behavior
- Location: Active Machine
- Data Source: System

[zhu2024honeyjudge] H. Zhu, M. Liu, B. Chen, X. Che, P. Cheng, R. Deng, Honeyjudge: A plc honeypot identification framework based on device memory testing, IEEE Transactions on Information Forensics and Security (2024)

Honeypot Detection in the Literature

Detection by Probing [chen2023honeypot]

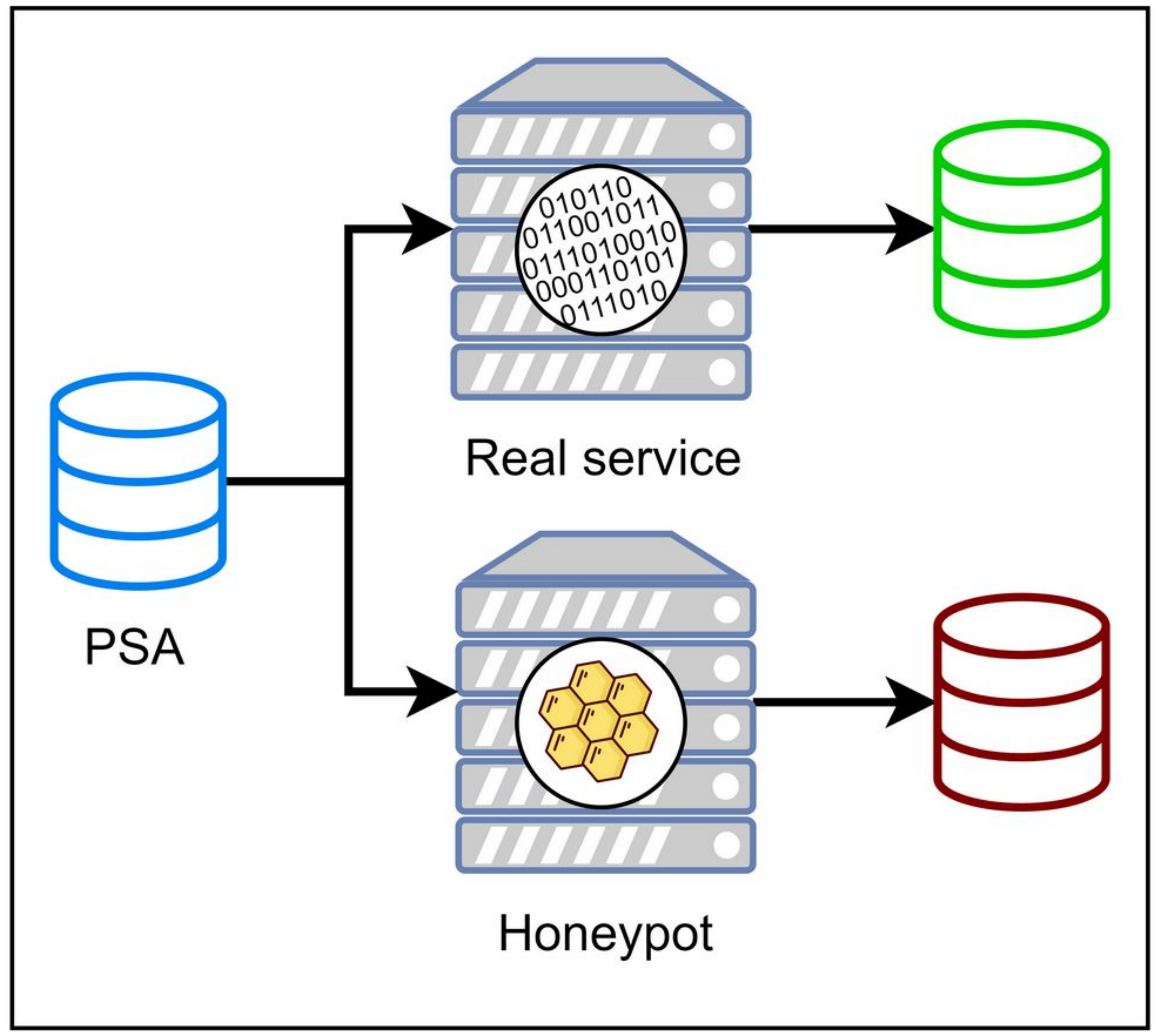


Fig.6: Probing packets Set based on Anomaly (PSA) property

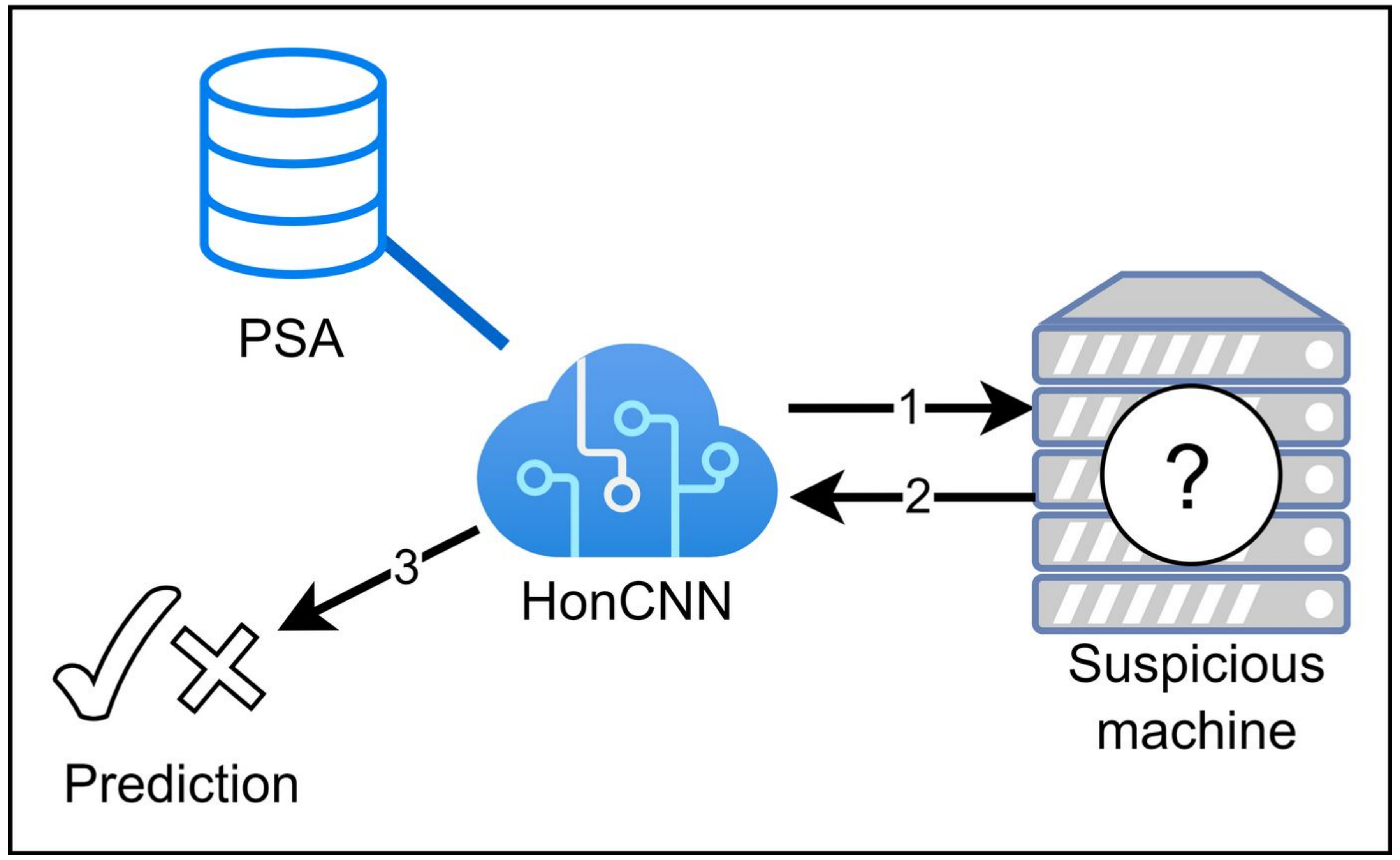


Fig.7: Convolution Neuronal Network for Honeypot detection

[chen2023honeypot] X. Chen, J. Andersen, Z. M. Mao, M. Bailey, J. Nazario, Towards an understanding of anti-virtualization and anti-debugging behavior in modern malware, in: 2008 IEEE international conference on dependable systems and networks with FTCS and DCC (DSN), IEEE, 2008, pp. 177–186.

Honeypot Detection in the Literature

Detection by Probing [chen2023honeypot]

[chen2023honeypot]
- Detection vector: Code
- Detection type: Fingerprint
- Location: Active Machine
- Data Source: Application

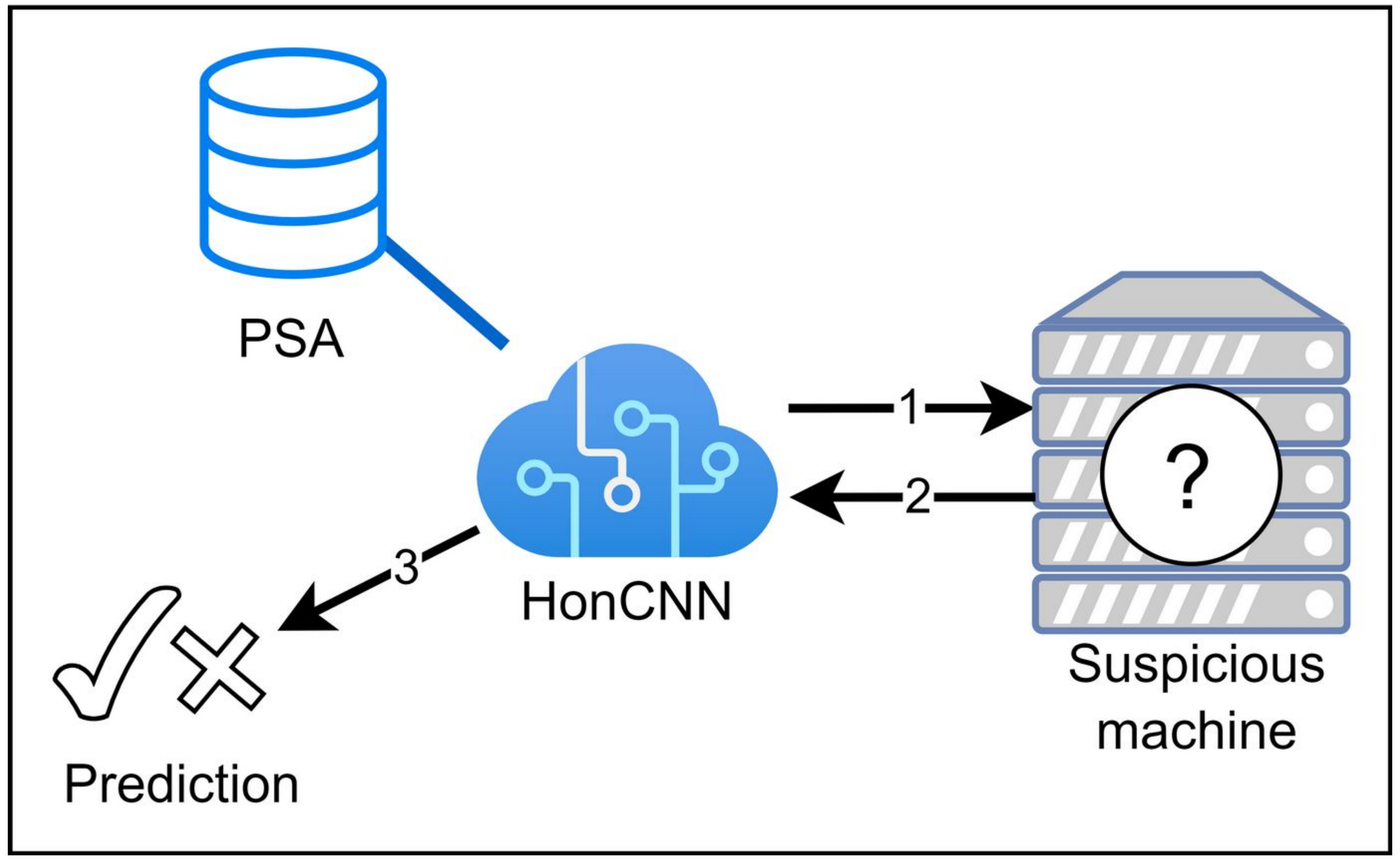


Fig.7: Convolution Neuronal Network for Honeypot detection

[chen2023honeypot] X. Chen, J. Andersen, Z. M. Mao, M. Bailey, J. Nazario, Towards an understanding of anti-virtualization and anti-debugging behavior in modern malware, in: 2008 IEEE international conference on dependable systems and networks with FTCS and DCC (DSN), IEEE, 2008, pp. 177–186.

Honeypot Detection in the Literature

Metrics I – 39 techniques / 20 papers

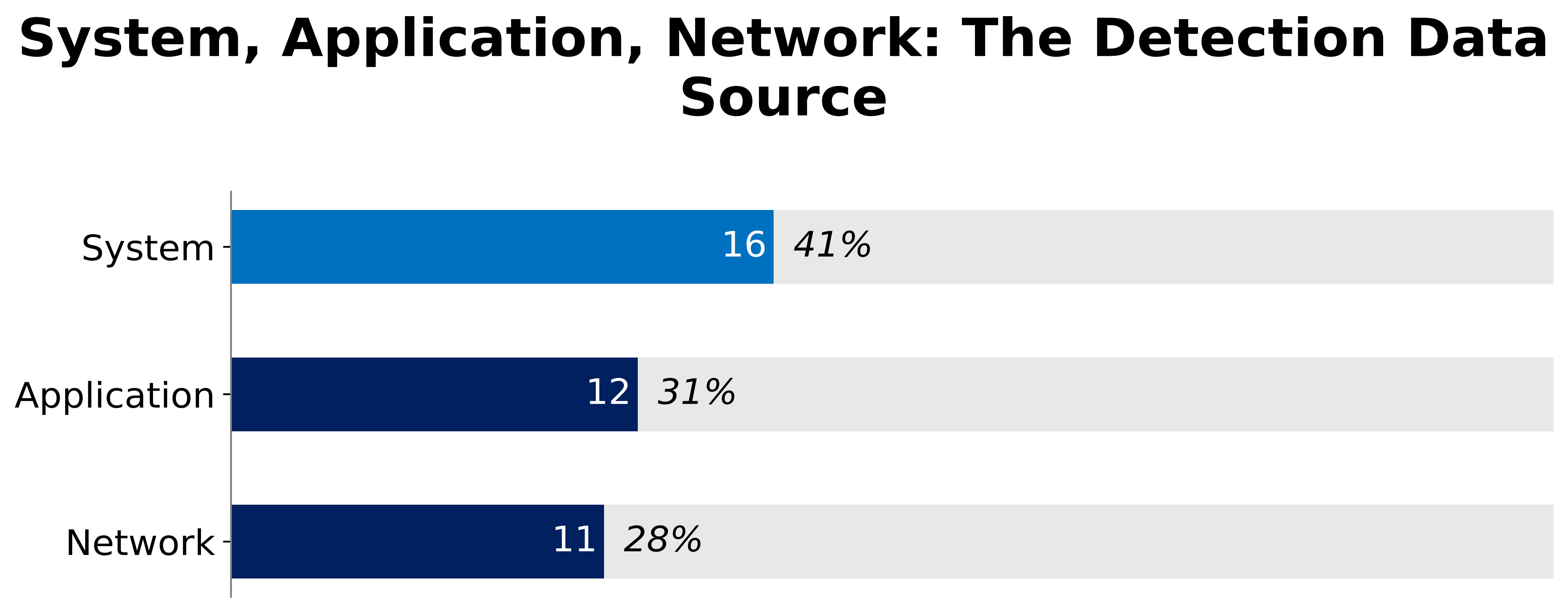


Fig.8: Data source of honeypot detection technique

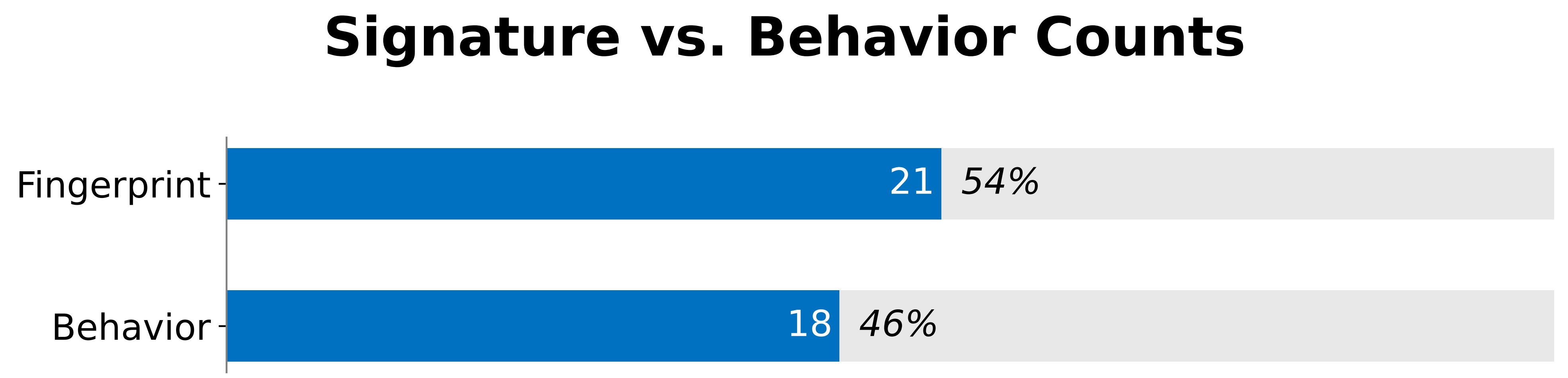


Fig.9: Type of honeypot detection technique

Honeypot Detection in the Literature

Metrics II – 39 techniques / 20 papers

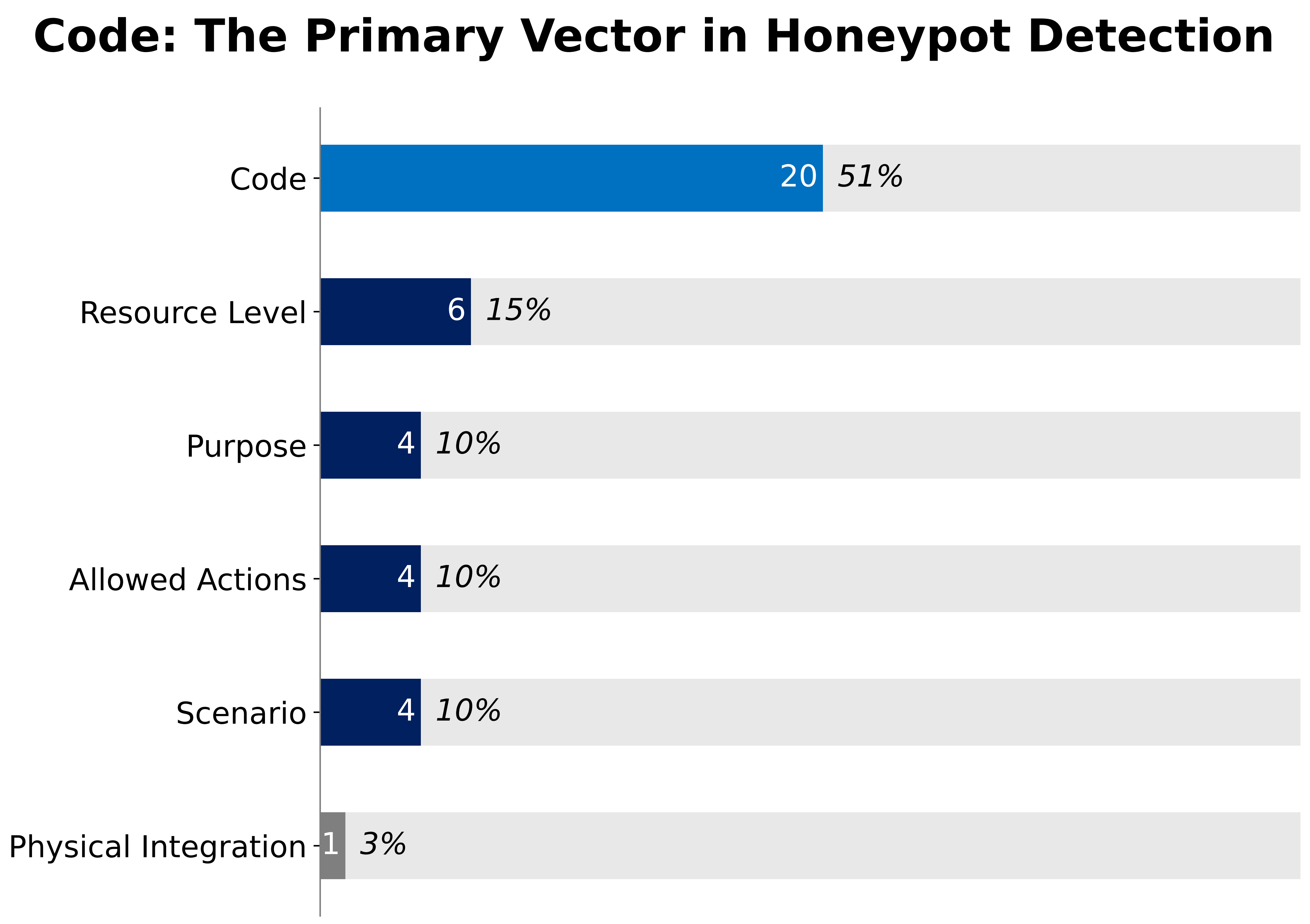


Fig.10: Vector of honeypot detection technique

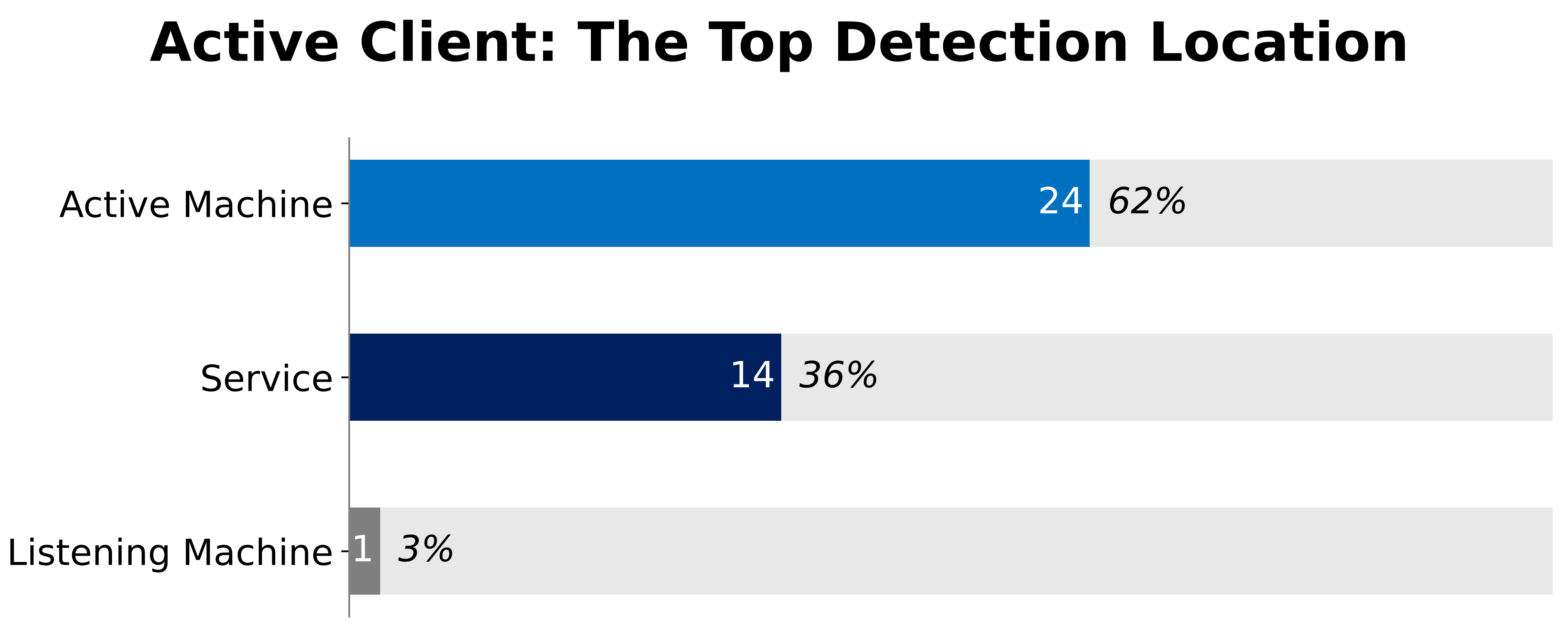


Fig.11: Location of honeypot detection technique

Honeypot Detection in the Literature

Metrics III – 39 techniques / 20 papers

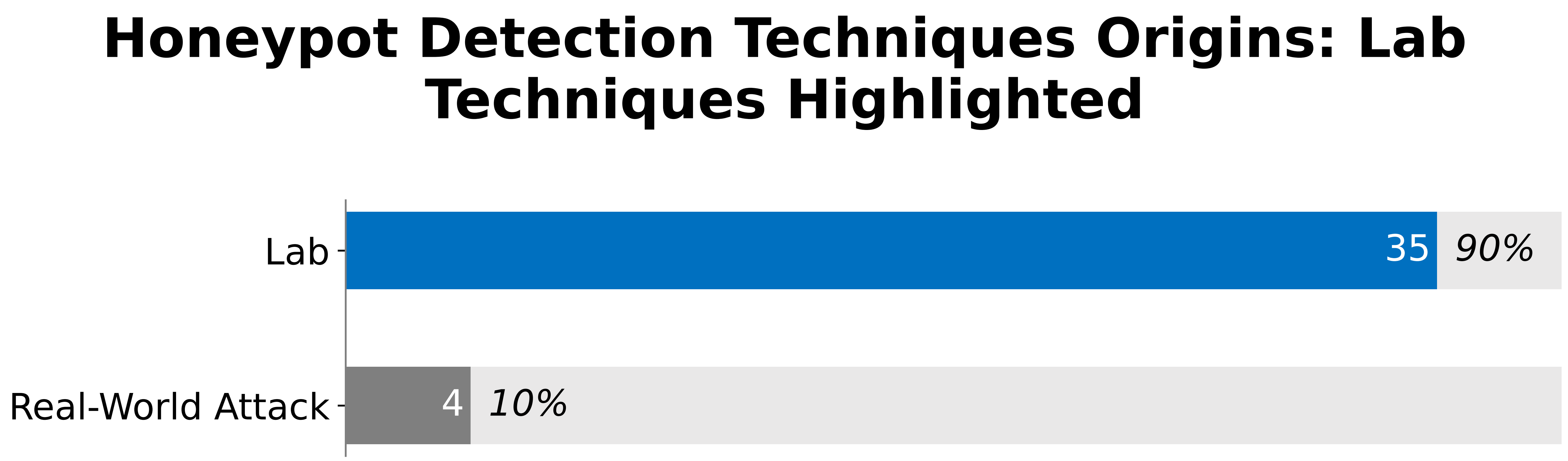


Fig.12: Origin of honeypot detection technique

3

Introduction
Motivation
Honeypot detection taxonomy
Detection techniques analysis
Mitigation

Mitigation

Key Actions

Customize the pot	System: hostname, apps, addresses App: banners, default responses
Upgrade the pot	Missing features Hidden honeypot intents
Build a scenario	User activity Appropriate security and accessibility

3

Takeaways

CHAIRE CYBER CNI
Sécurité des infrastructures critiques

Takeaways

Dominant detection properties

Origin	Lab
Category	Operations / Environment
Vector	Code
Type	Fingerprint / Behavior
Data source	Application / System / Network
Location	Active Machine / Service

My presentation in a nutshell

Motivation

Related work

Reference	Year	Taxonomy	Strategy: Evasion	Strategy: Detection	Type: Fingerprint	Type: Behavior	Origin: Lab	Origin: Attack
[chen2008towards]	2008	◐	●		●	●		●
[lauren2017survey]	2017	◐		●	●		●	
[afianian2019survey]	2019	◐	●				●	●
[tay2023taxonomy]	2023	◐		●	●		●	
Our SoK	2025	●	●	●	●	●	●	●

[chen2008towards] X. Chen, J. Andersen, Z. M. Mao, M. Bailey, J. Nazario, Towards an understanding of anti-virtualization and anti-debugging behavior in modern malware, in: 2008 IEEE international conference on dependable systems and networks with FTCS and DCC (DSN), IEEE, 2008, pp.177–186.
[lauren2017survey] S. Laurén, V. Leppänen, S. Rauti, J. Uitto, A survey on anti-honeypot and anti-introspection methods, Recent Advances in Information Systems and Technologies 2 (2017) 11–13.
[afianian2019survey] A. Afianian, S. Niksefat, B. Sadeghiyan, D. Baptiste, Malware dynamic analysis evasion techniques: A survey, ACM Computing Surveys (CSUR) 52 (2019) 1–28.
[tay2023taxonomy] V. Tay, X. Li, D. Mashima, B. Ng, P. Cao, Z. Kalbarczyk, R. K. Iyer, Taxonomy of fingerprinting techniques for evaluation of smart grid honeypot realism, in: 2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), IEEE, 2023, pp. 1–7.

Honeypot Detection in the Literature

Detection by Memory Testing [zhu2024honeyjudge]

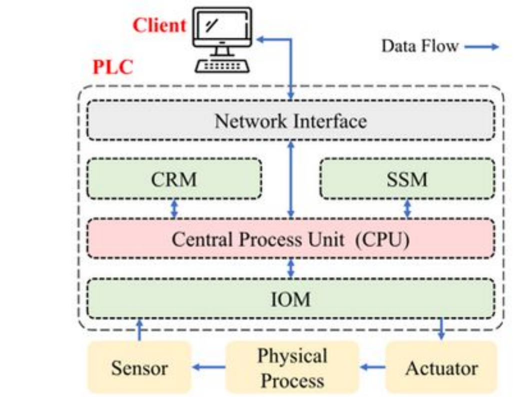


Fig.5: The memory architecture and connection within the PLC

[zhu2024honeyjudge]
- Detection vector: Resource Level
- Detection type: Behavior
- Location: Active Machine
- Data Source: System

[zhu2024honeyjudge] H. Zhu, M. Liu, B. Chen, X. Che, P. Cheng, R. Deng, Honeyjudge: A plc honeypot identification framework based on device memory testing, IEEE Transactions on Information Forensics and Security (2024)

Mitigation

Key Actions

Customize the pot	System: hostname, apps, addresses App: banners, default responses
Upgrade the pot	Missing features Hidden honeypot intents
Build a scenario	User activity Appropriate security and accessibility No Virtual Machine if not relevant

Takeaways

Dominant detection properties

Origin	Lab
Category	Operations / Environment
Vector	Code
Type	Fingerprint / Behavior
Data source	Application / System / Network
Location	Active Machine / Service

3

CHAIRE

CYBER CNI

Sécurité des infrastructures critiques