Center for Reverse Engineering and Assured Microelectronics (CREAM)

MUD at Morgan

Khir Henderson
Edmund Smith, Paige Harvey, Tsion Yimer, Otily Toutsop, Sean Richardson

Dr. Kevin Kornegay - Advisor

Introduction

High Priority Issues

Reduce

Threat of network compromises due to:

- outdated firmware
- weak security practices

Prevent

Large scale coordinated network attacks

- Distributed Denial of service (DDOS)

Internal network attacks

- Access and Privilege Escalation

Protect

Homogenous IoT networks at scale

- Internal
- External

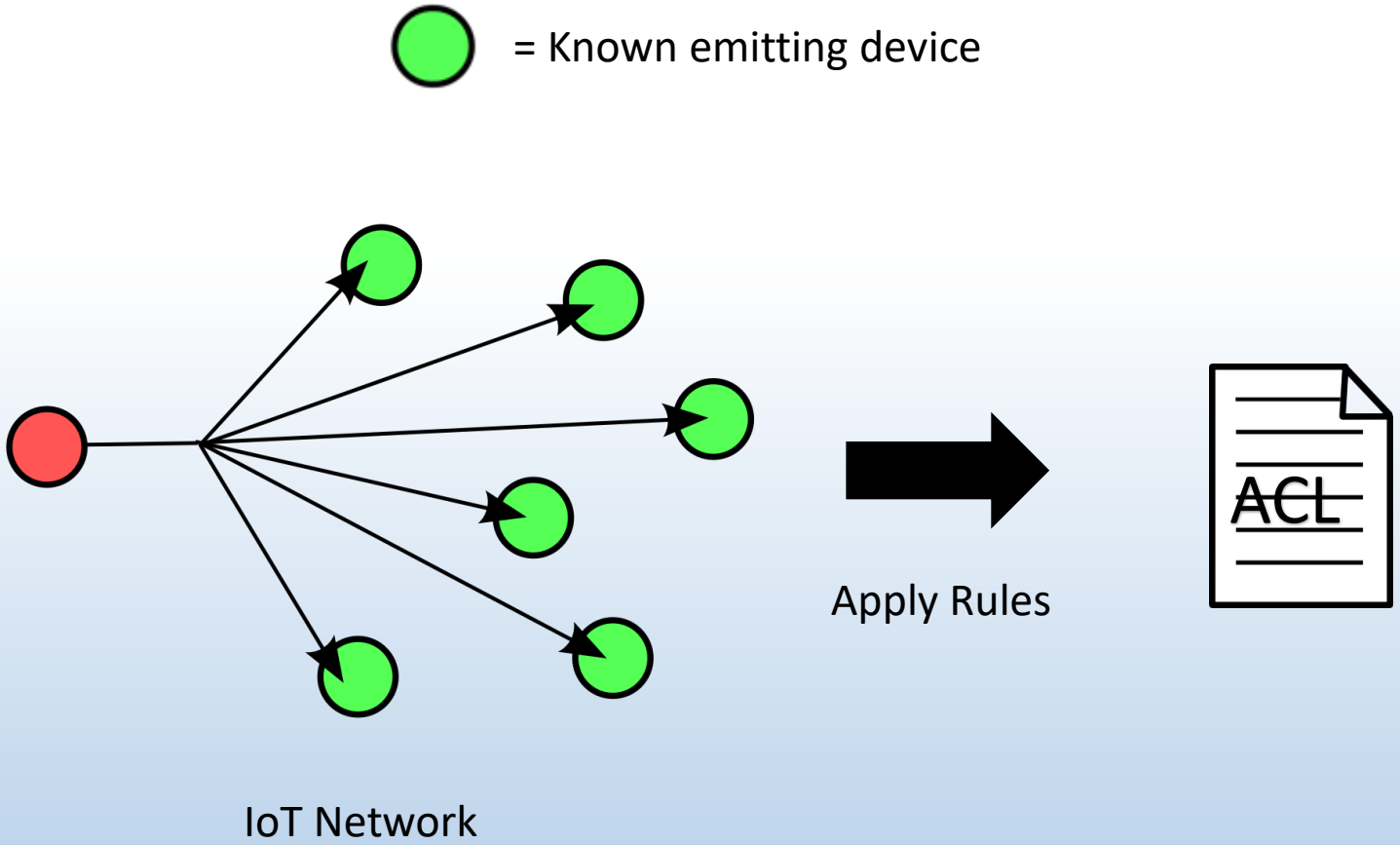
Manufacture Usage Description (MUD)

What we like

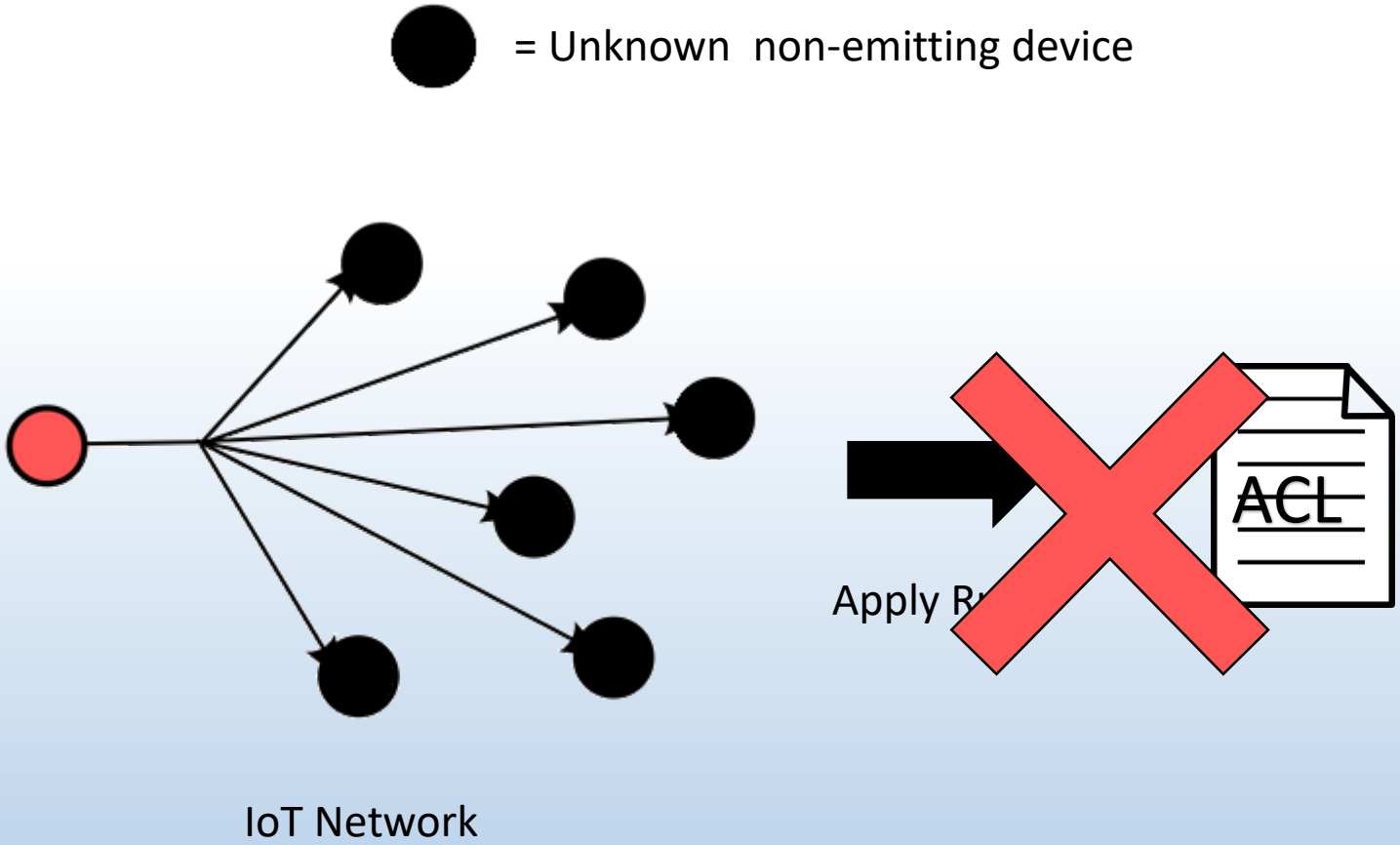
- Automation and Scalability
- Security as a standard
- Modernized NACLs
- Distributed root of trust
- Onsite and active security

Our Thoughts and Research

Our Thoughts & Research



Our Thoughts & Research



Our Thoughts & Research

Device Identification

Device Fingerprinting

Device Profiling

- Device fingerprinting attempts to use identifying characteristics such as packet header data to make an informed guess on the identity of a device.

SHODAN

censys

Our Thoughts & Research

Device Identification

Device Fingerprinting

Device Profiling

- Device profiling methods attempt to learn the network patterns of a device to create a behavioral profile that can be used to identify the device

MUD*gee*

[1] *MUD: Generating, Validating and Applying IoT Behaviorial Profiles (Technical Report) Ayyoob Hamza∗, Dinesha Ranathunga†, H. Habibi Gharakheili∗ Matthew Roughan∗ and Vijay Sivaraman*

Our Thoughts & Research

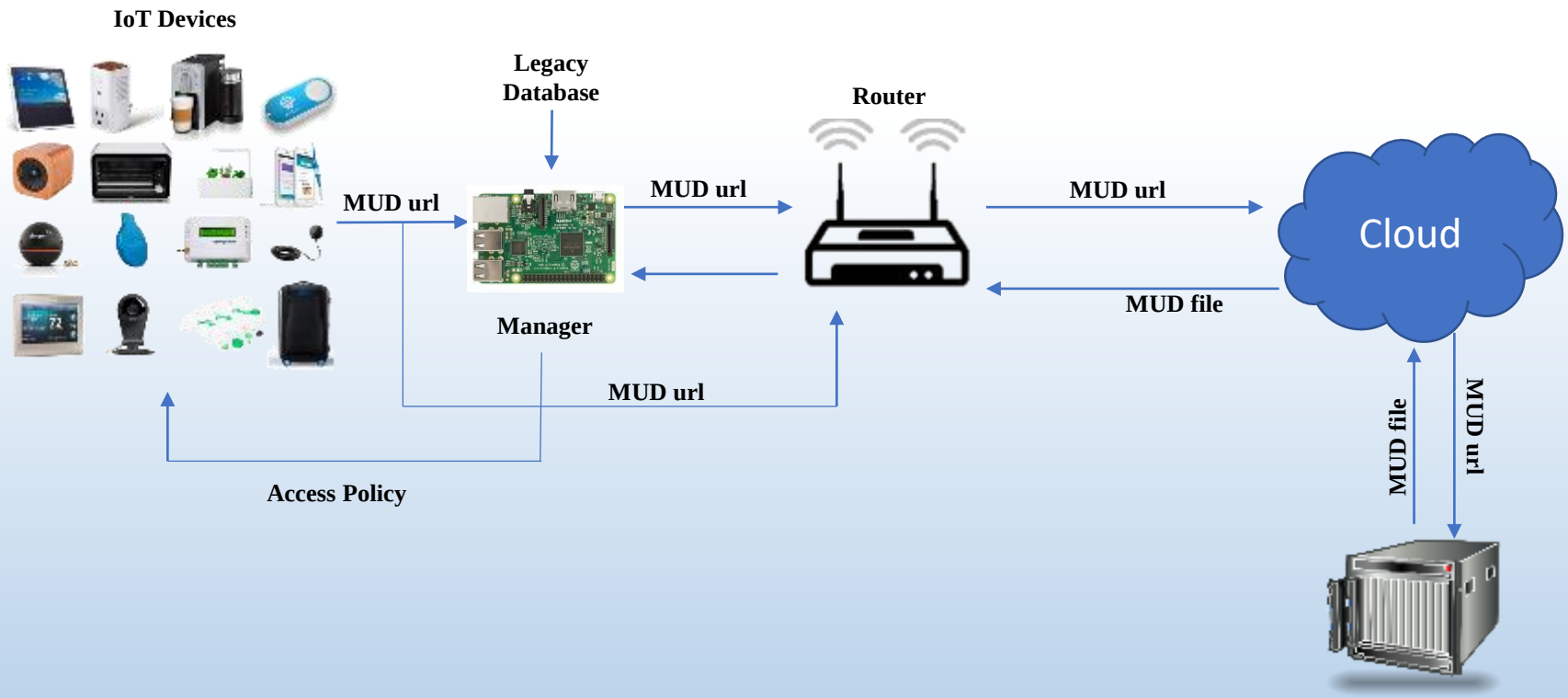
Device Identification

Our Work: Compare device identifying methods

- Further define and diagram methods:
  - Fingerprinting
  - Profiling
- Model the efficiency of each method for scaled networks
- Theoretically determine efficacy for differing network use cases
- Contribute towards application of access control of legacy devices

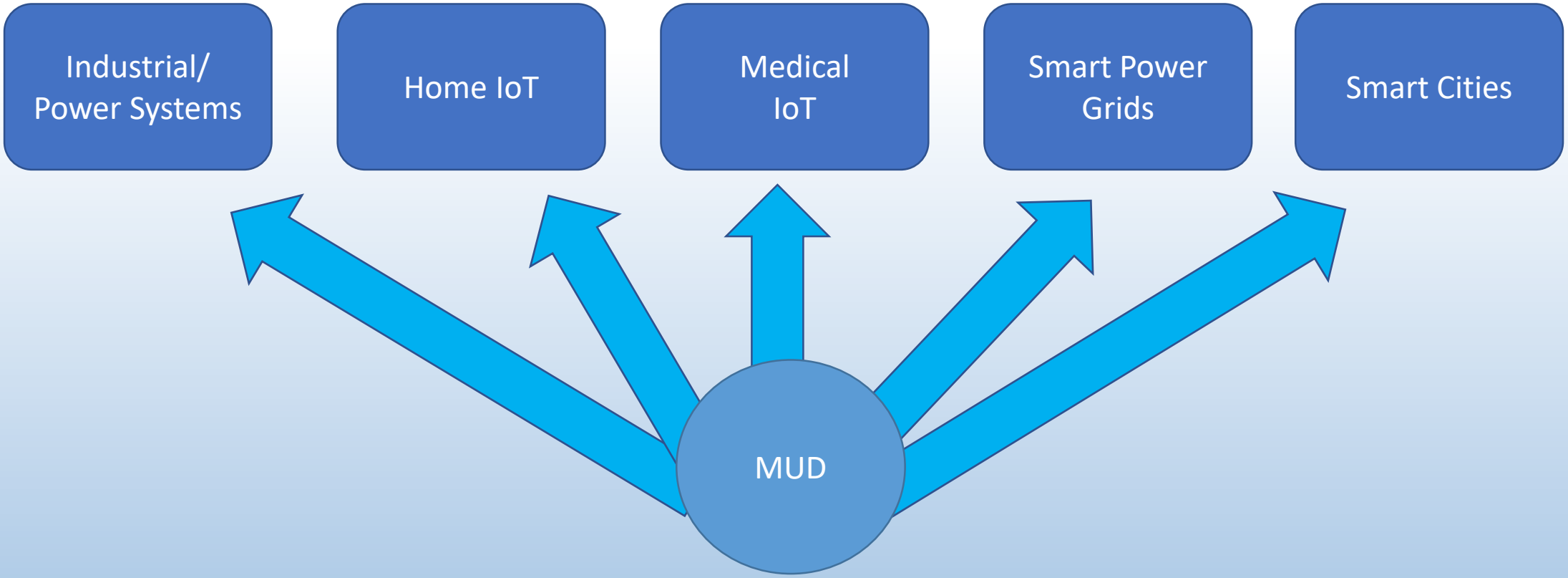
Our Thoughts & Research

Implementation



Our Thoughts & Research

Implementation



Our Thoughts & Research

Implementation

- Full scale penetration test
  - Internal (local) access attacks
    - Open port vulnerabilities
    - Device vulnerabilities
    - Default Passwords
  - External (public) access Attacks
    - Open port
- Infrastructure security
  - Certificate Authority
  - Transmission Protocols
  - MUD database
- Man – In-the middle attacks
- Spoofing attacks
- DNS Based attacks
- Scalability with firewalls
- Etc.

Our Thoughts & Research

Implementation

Results

Reveal

- Key vulnerabilities
- Strengths per use-case scenario

Present

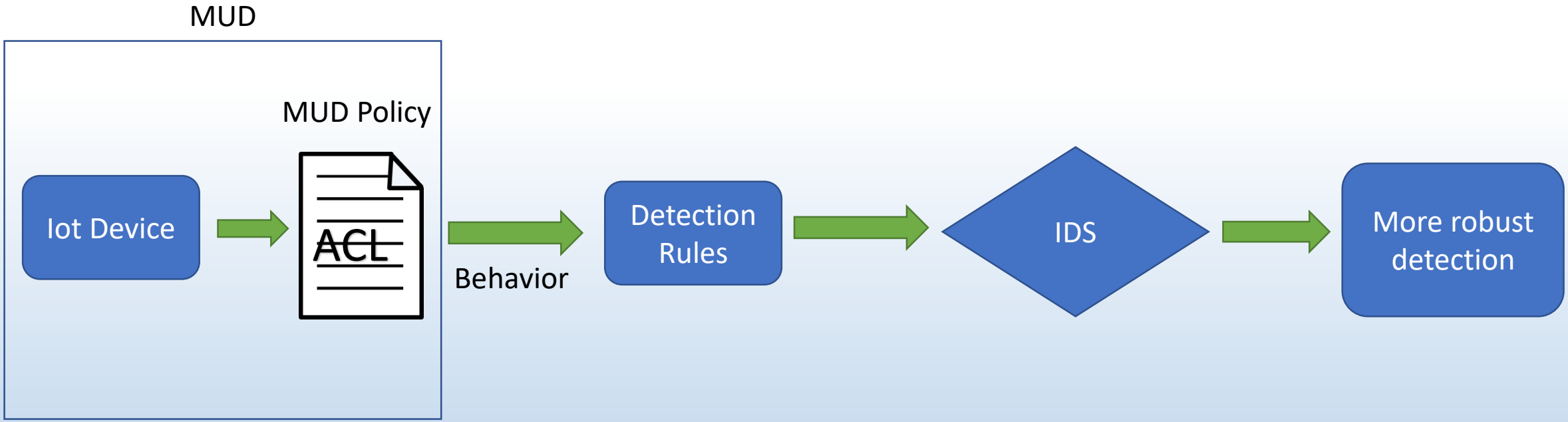
Best Practices

Provide

Theoretical risk assessments for network attacks per each use-case

Our Thoughts and Research

Intrusion Detection and Prevention



Our Thoughts & Research

Future Landscape

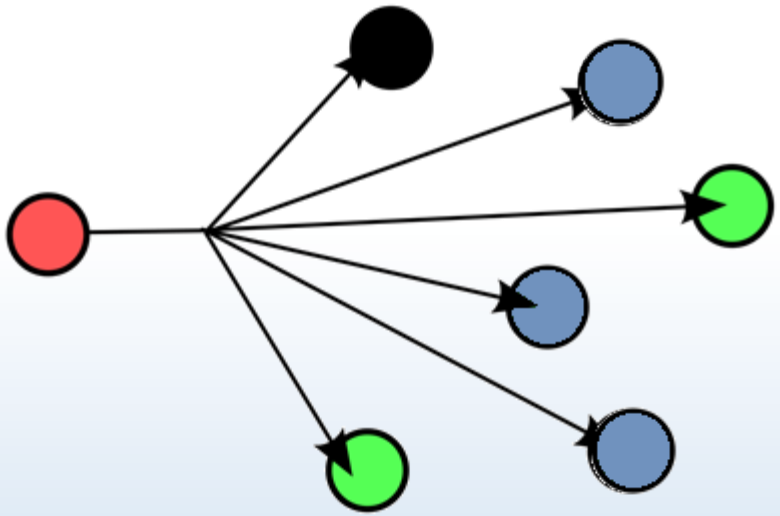
- Commercial and Public implementations of MUD
- Open source network managers such as Pi-Hole
- Open source custom router software

OpenWrt
Wireless Freedom

Pi-hole®

Our Thoughts & Research

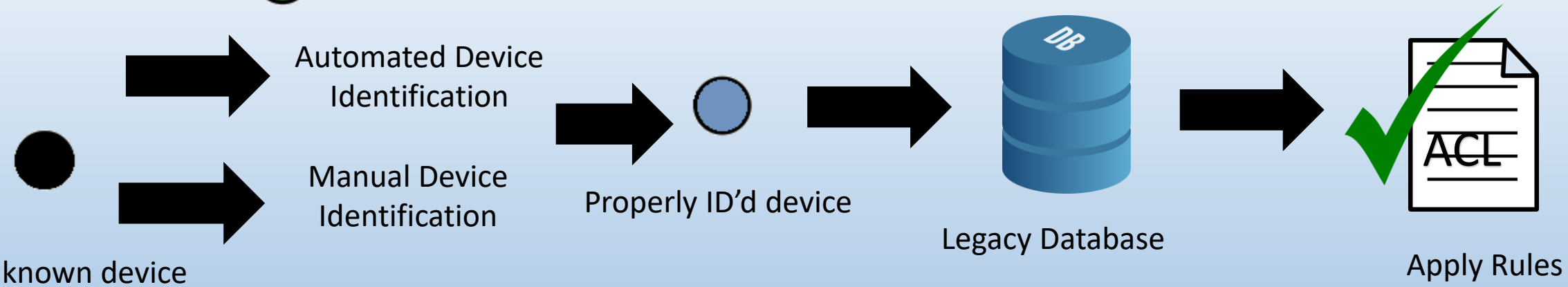
Heterogenous IoT Network



= Known emitting device

= Unknown non-emitting device

= Identified non-emitting device



Our Thoughts and Research

MUD at Morgan

- Suitable Device Identification
- Scale Hardware implementation testbed
- Security evaluations and penetration test
- MUD in different use cases
- MUD synergy with IDS
- Public and commercial implementations of MUD

Thank You

Thanks

- Dr. Kevin Kornegay
- Dr. Donna Dodson
- Dr. Murugiah Souppaya
- MSU Colleagues
- NCCOE & NIST
- IETF
- CISCO
- MUD Authors and Developers
  - Elliot Lear, Ralph Droms, Dan Romascanu, Rashmikant Shah, Brian Weis, Cheryl Madson

Thank You again!

Comments, Ideas, Questions?