

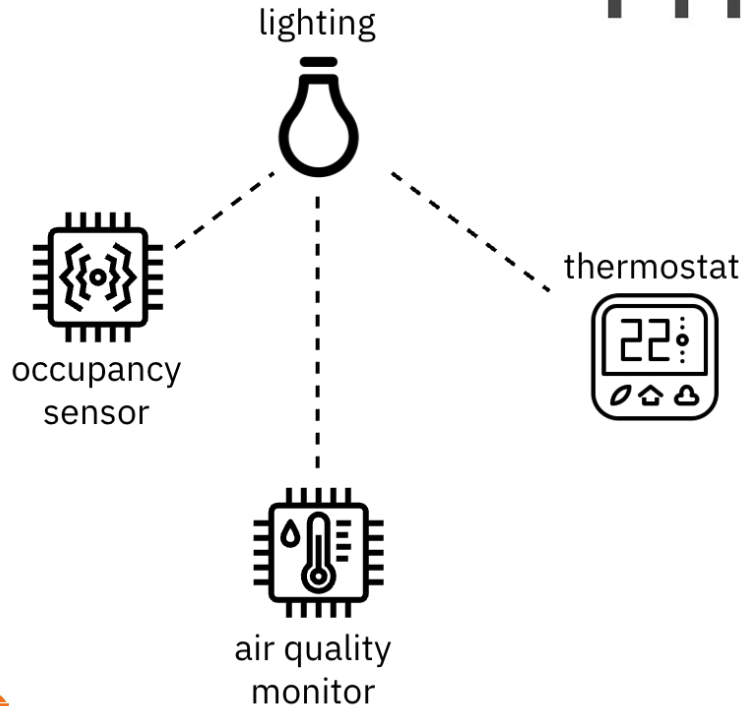
Isle: Network-level Isolation for Low-Power Embedded Applications

Marshall Clyburn, University of Virginia

Brad Campbell, University of Virginia

Thread for local, low-power wireless

THREAD



Low-barrier, extensible connectivity.

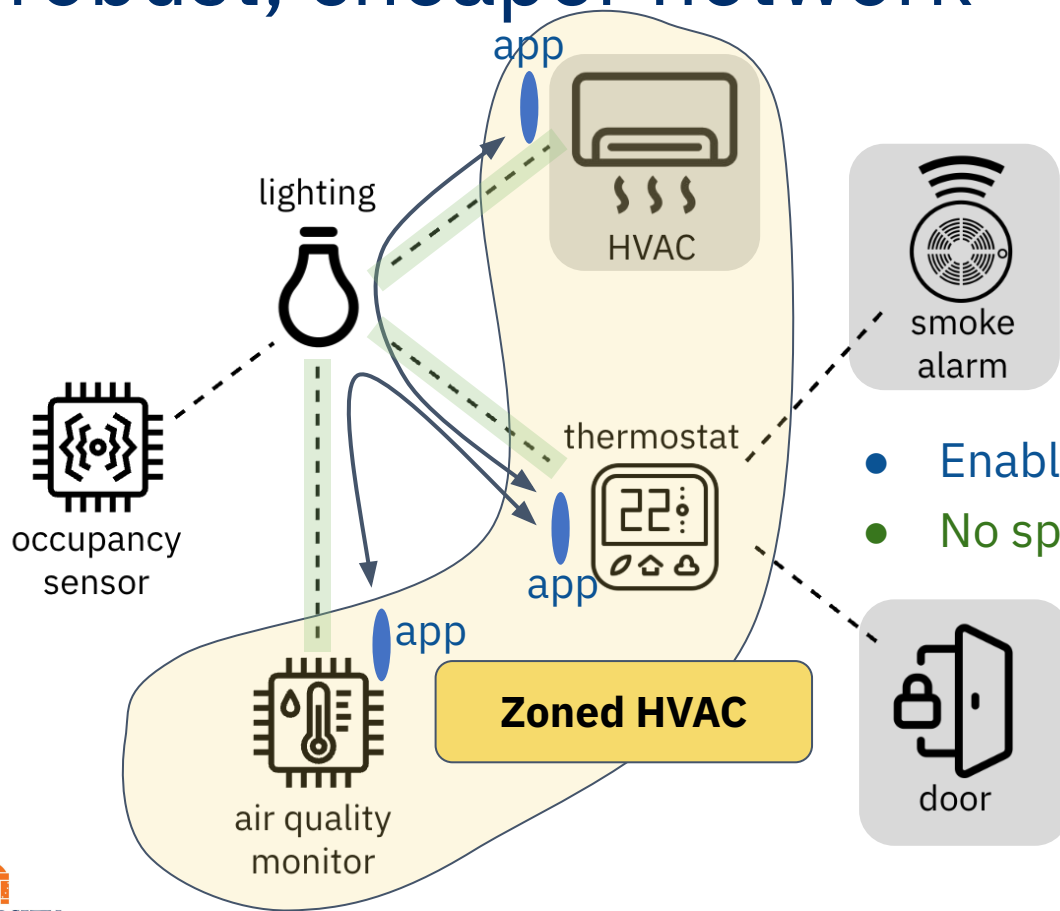
IPv6

Familiar, compatible networking.



Energy-efficient, low-power operation.

A robust, cheaper network



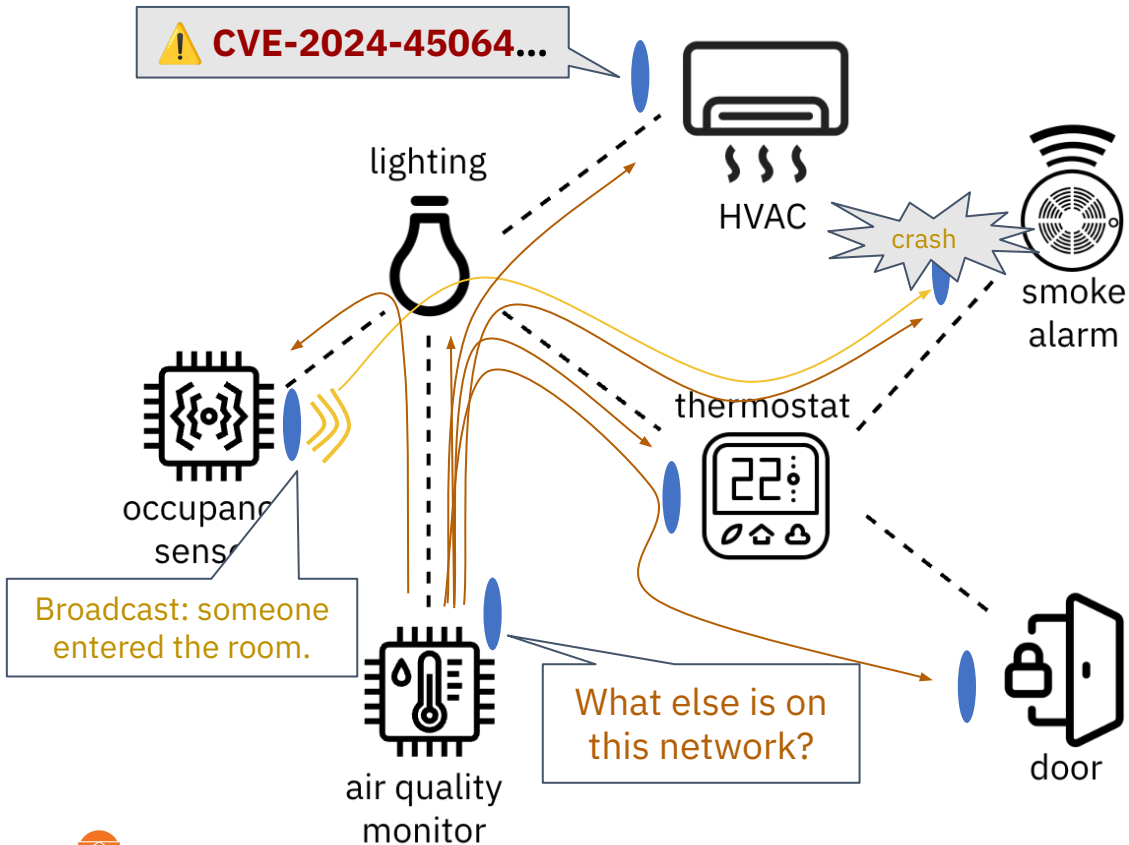
**Thread connectivity
is expanding.**

- Enables powerful IoT applications.
- No specialized gateway hardware.

A robust, cheaper network?



CVE-2024-45064...

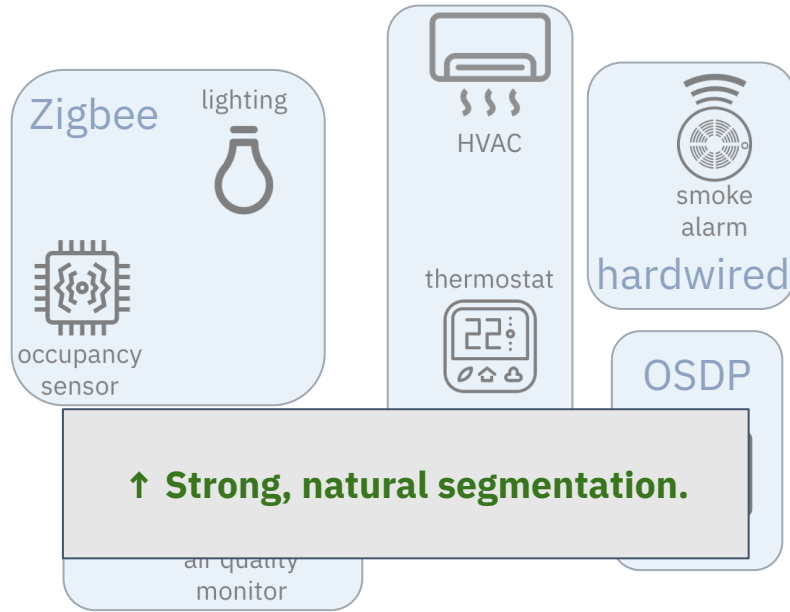


Applications are **buggy**...

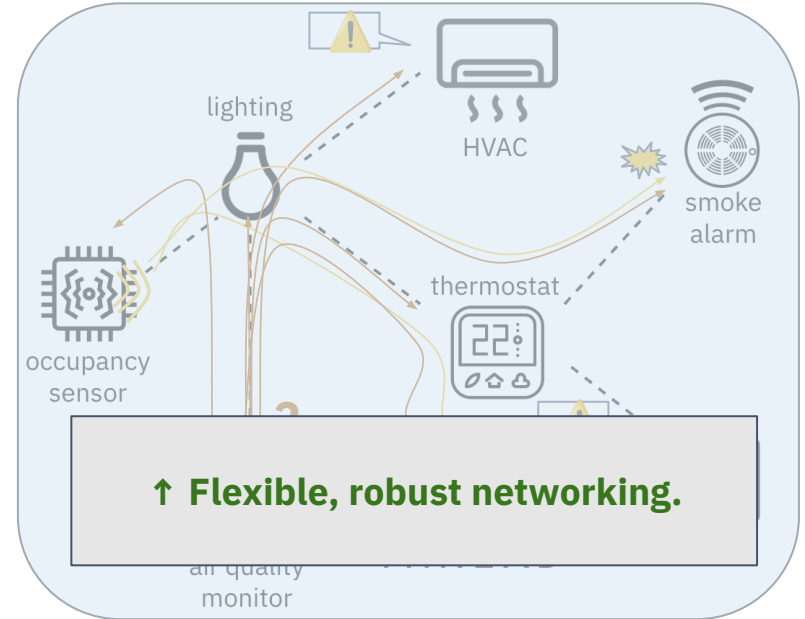
...some are even **suspect**...

...and some possess **known and unknown vulnerabilities**.

Connectivity has eroded **isolation**



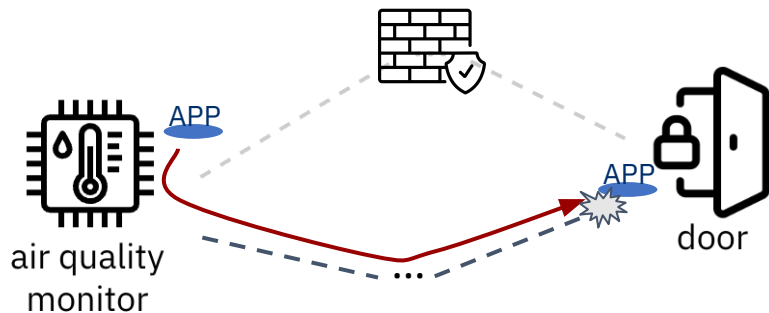
Networking technology heterogeneity
creates isolation.



Unified mesh networking
erodes isolation.

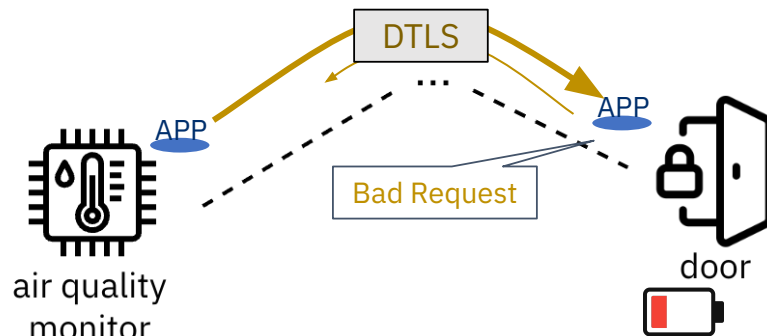
Non-solutions for application isolation

Firewalls and VLANs



Eventually circumvented by dynamic network structure.

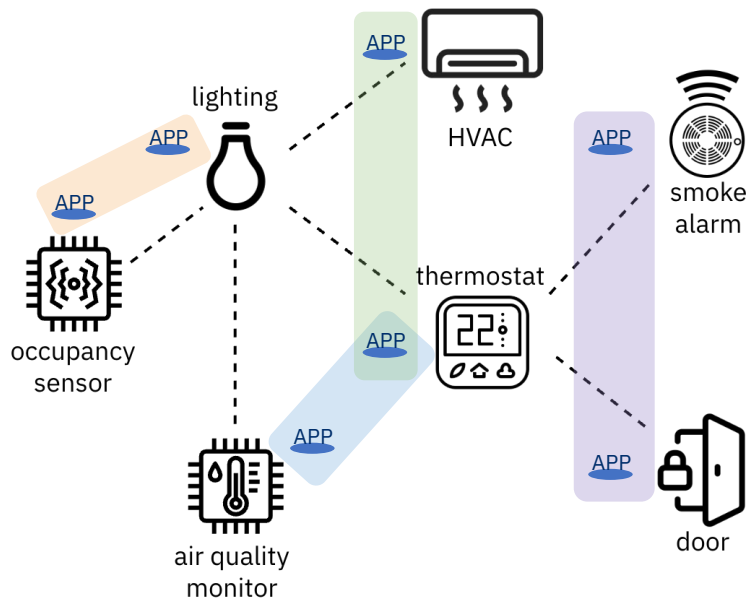
Application-layer security



Even a *correct* response wastes resources.

Effective isolation in the embedded mesh

Constrain **application-layer activity**, not device connectivity.

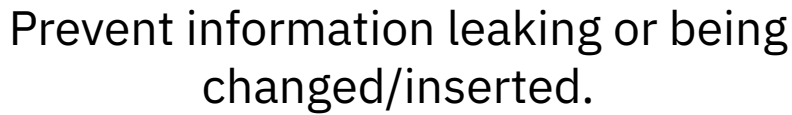


Add a new network layer for isolation?

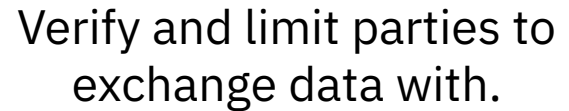
- Minimize frame size overhead.
- Maintains low processing overhead.

UNIVERSITY
of VIRGINIA

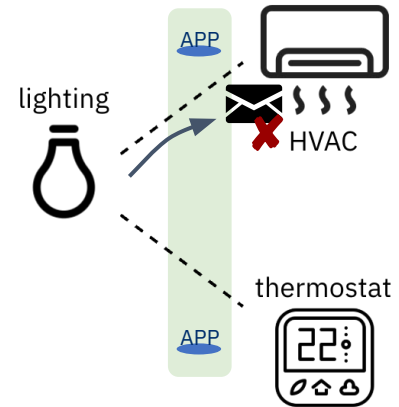
encryption



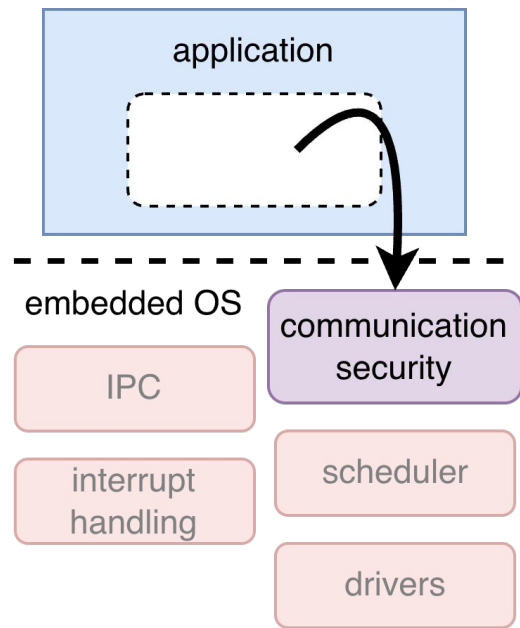
integrity



authentication



Key idea: move cryptography out of the application



Instead of adding an entirely new layer, **reuse application-layer security** to also provide isolation.

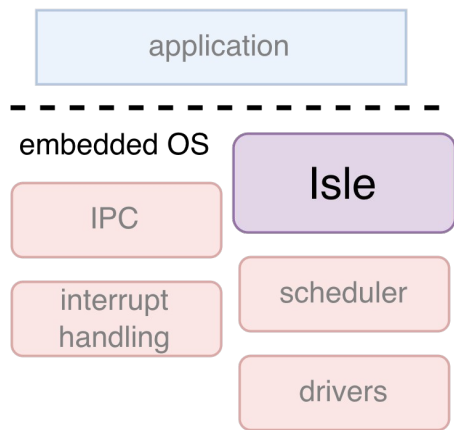
Moving communication security into the OS enables **enforceable** network isolation.

- Controlling keys, IVs limits connections.

Reusing application-layer security avoids the overhead of an entirely new layer.

Isle, an OS facility for application network isolation

Isle is an on-device, OS-level facility filtering application traffic to enforce network-level isolation.



G1 Segment applications, not the mesh.

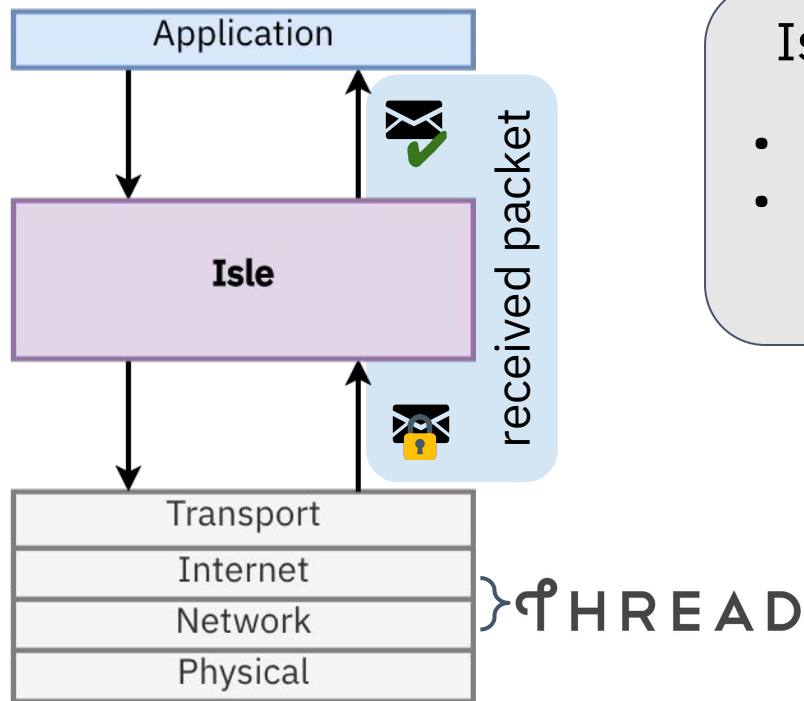
G2 Maintain low latency and frame size overheads.

G3 Operate transparent to the application.

Provide compatibility with CoAP-based protocols.

Enable cryptographic agility.

Constraining application network traffic

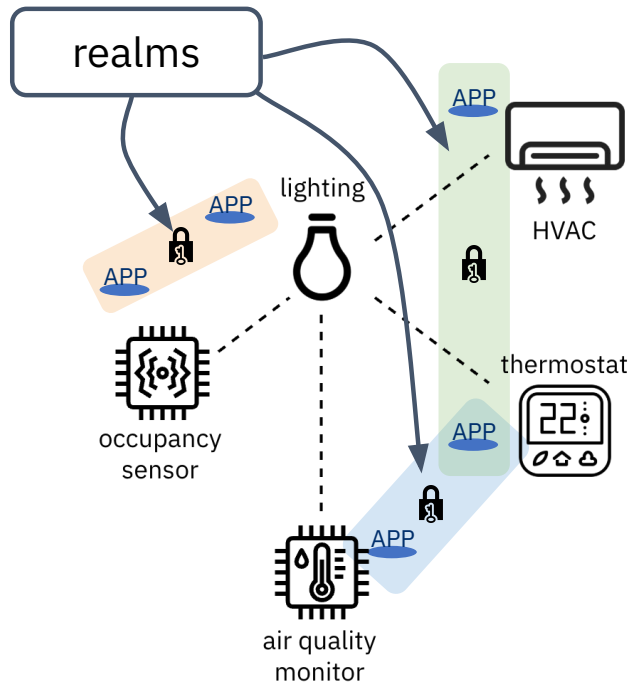


Isle runs as part of the network stack.

- Provides application-layer security.
- Decides which packets to pass.

Isle controls application network traffic flow without impacting mesh connectivity.

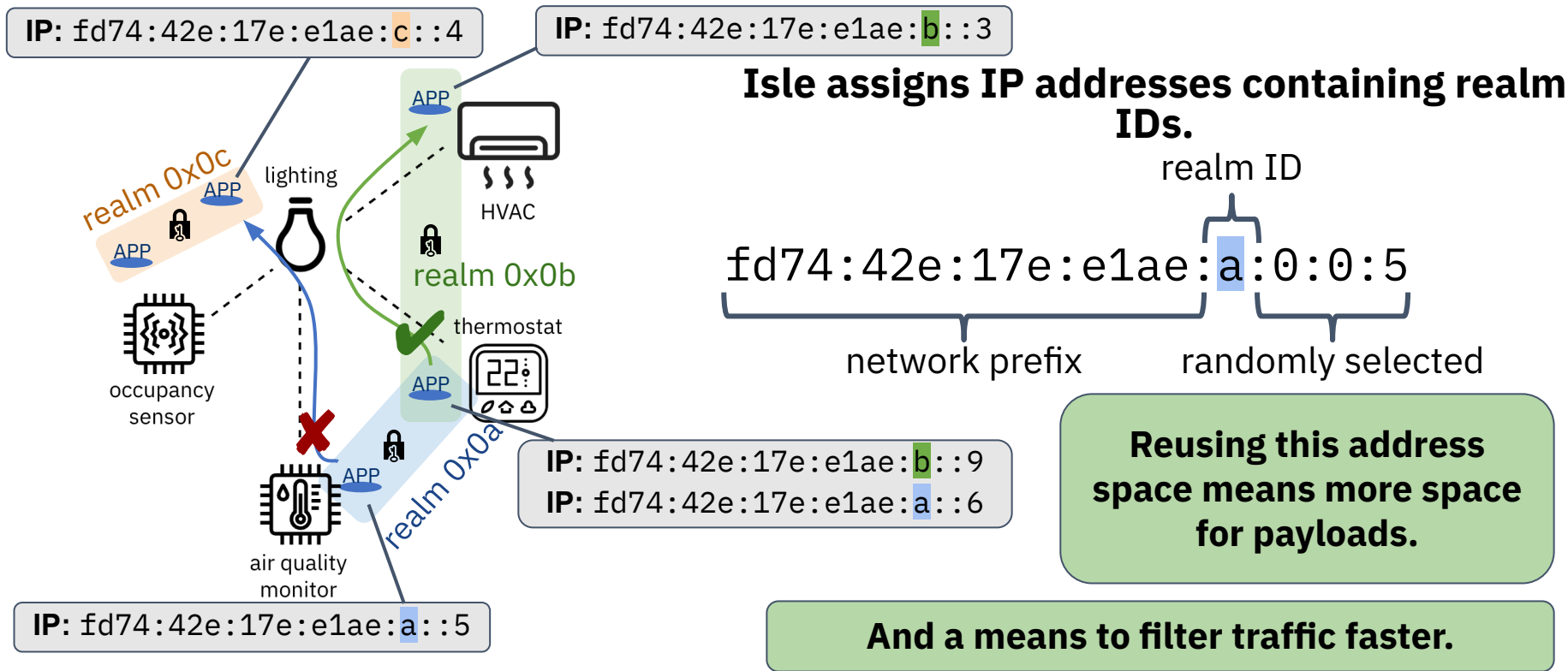
Isolating applications with **realms**



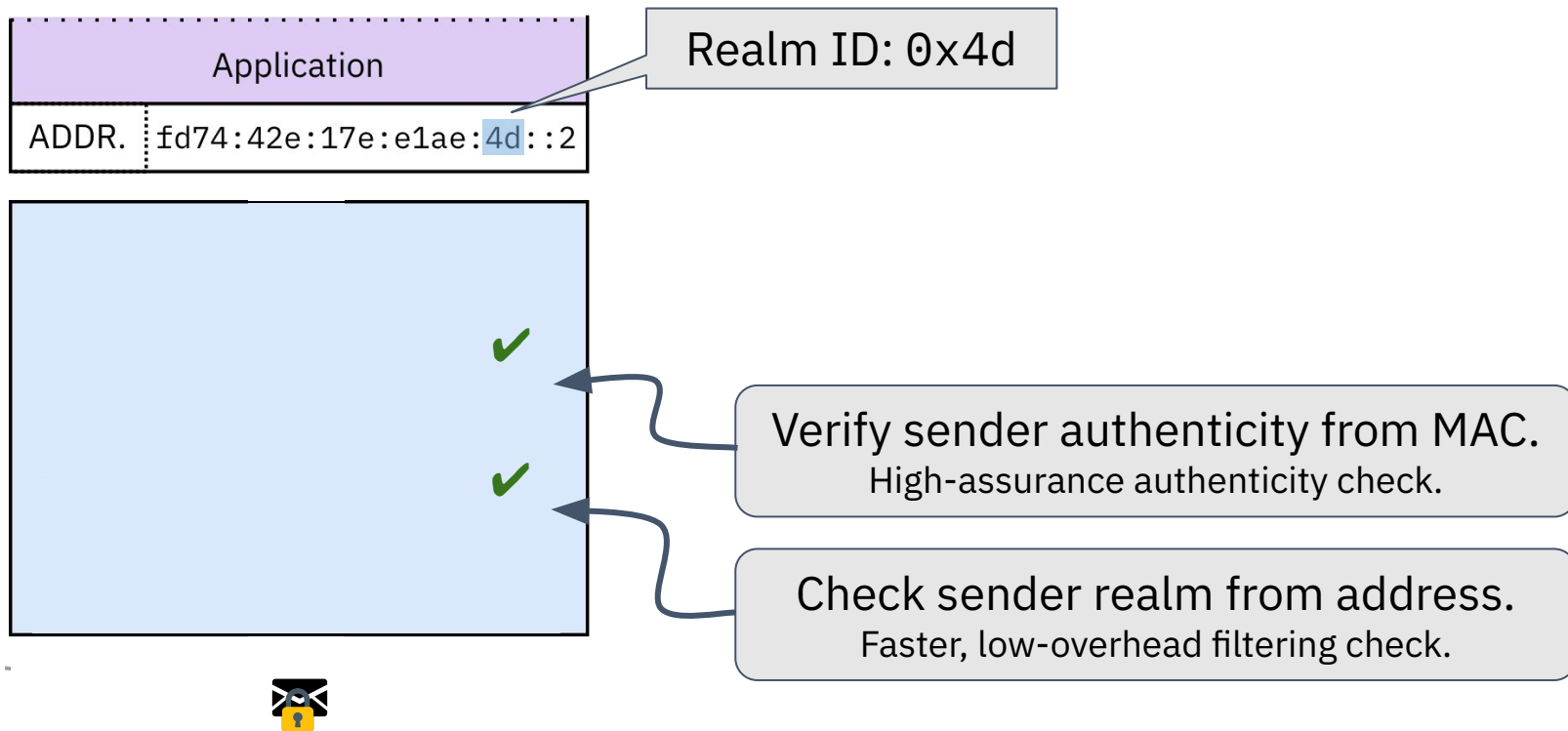
realm: set of mutually reachable applications.

- Realms share cryptographic parameters.
- Secure 1-to-1 and 1-to-many communication.
- Only in-realm communication allowed.

Tagging packets for realms



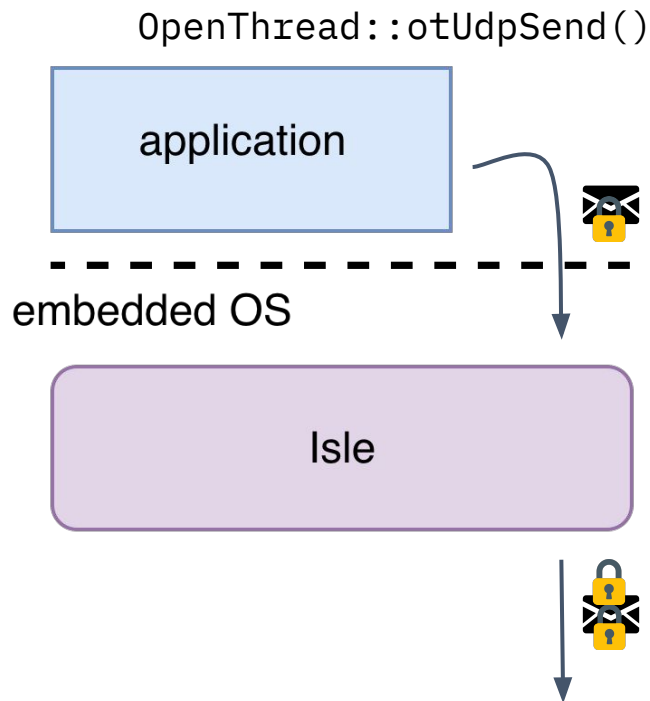
Processing application traffic with Isle



G2

Maintain low latency and frame size overheads.

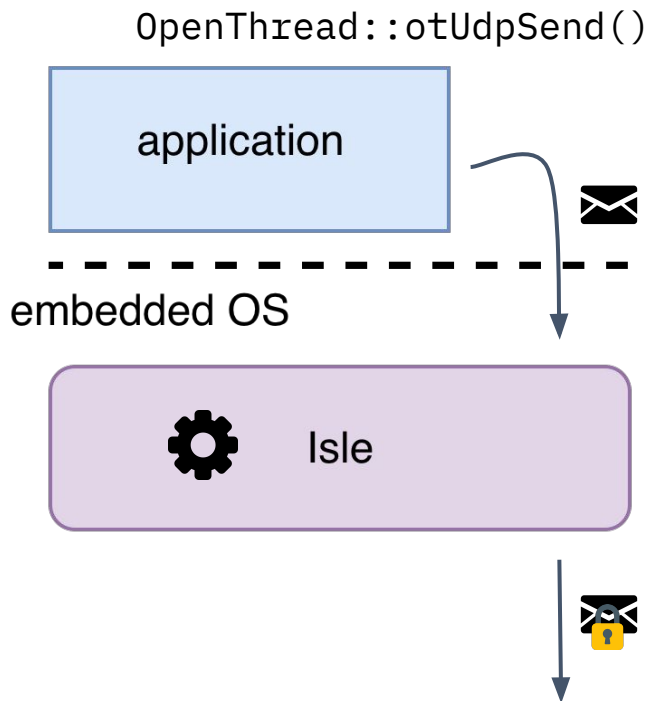
Application-side operation with Isle



Application-side

- Isle works transparently; no deep integration.
 - Even an existing application will work.
- Full benefit: remove application-layer security.
 - Reduces code size for multi-tenant devices.
- No networking API usage changes.

System-side operation with Isle



Application-side

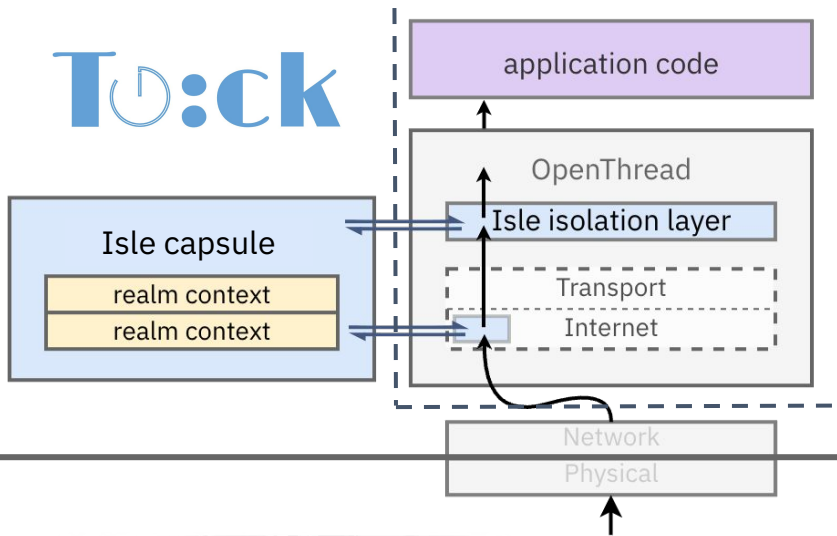
- Isle works transparently; no deep integration.
 - Even an existing application will work.
- Full benefit: remove application-layer security.
 - Reduces code size for multi-tenant devices.
- No networking API usage changes.

System-side

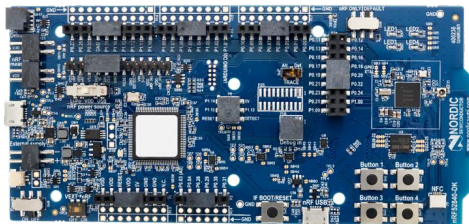
- Exposes configuration for system owner.
- Enforces isolation with no control API.

Building and testing Isle

Tock

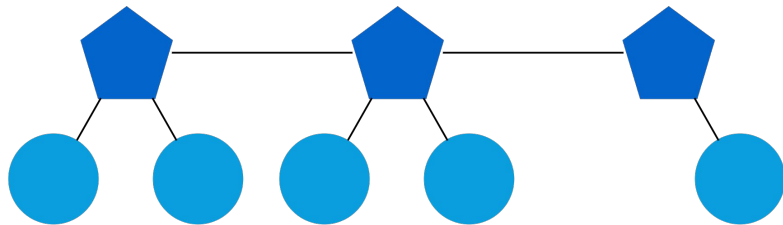


- Build as an OS module in Tock OS.
- Isle coordinates with the network stack.
- Eight networked nRF52840dk boards.
- Five end devices, running Isle on Tock.
- Three router devices.



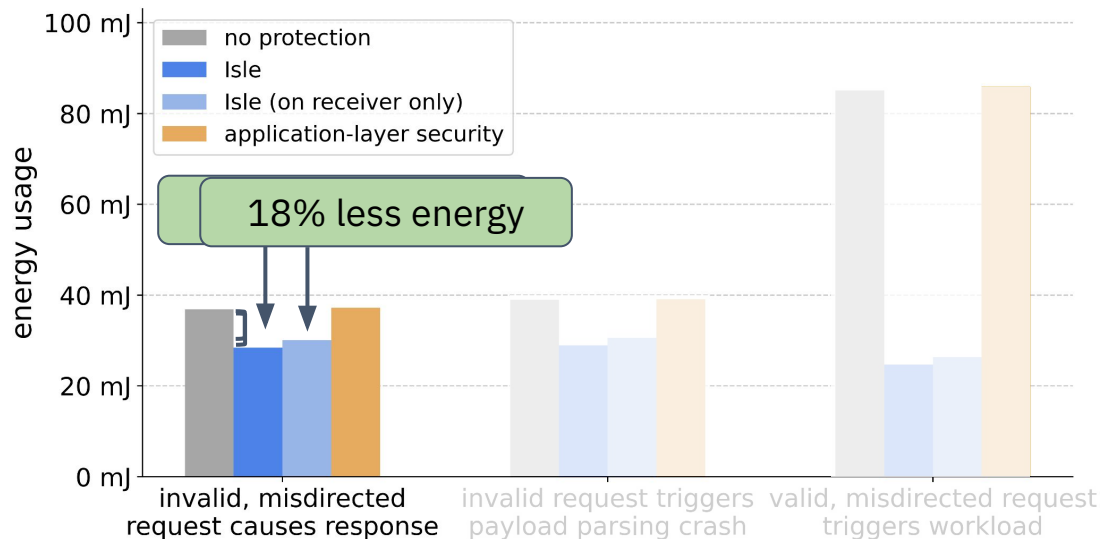
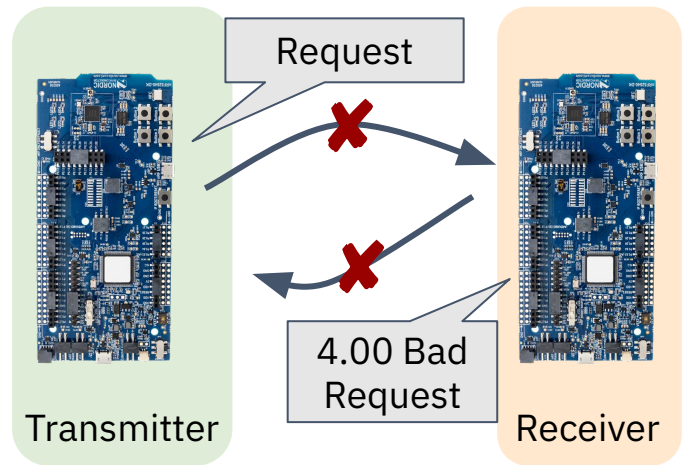
x8

routers
end devices



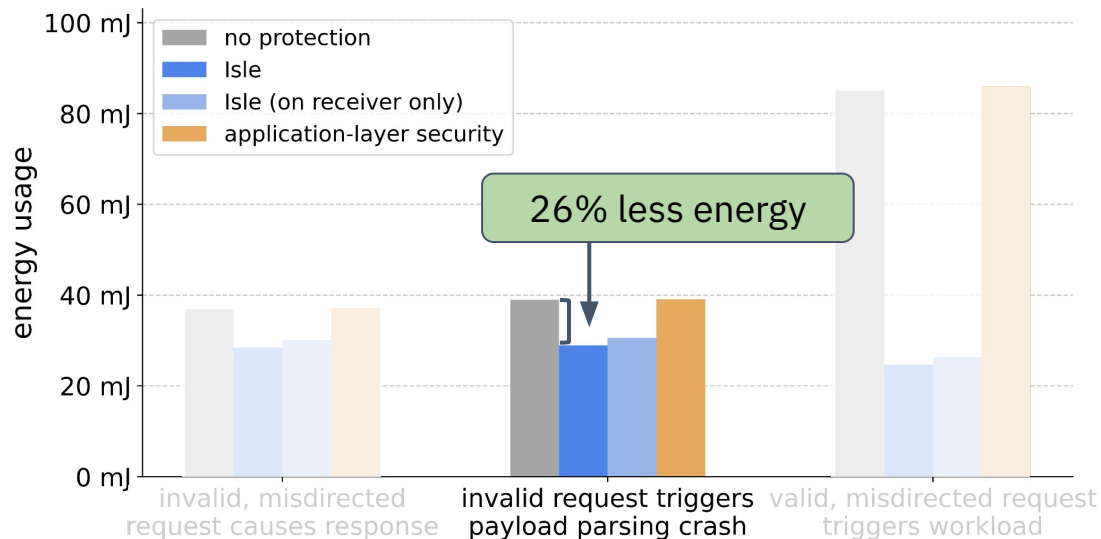
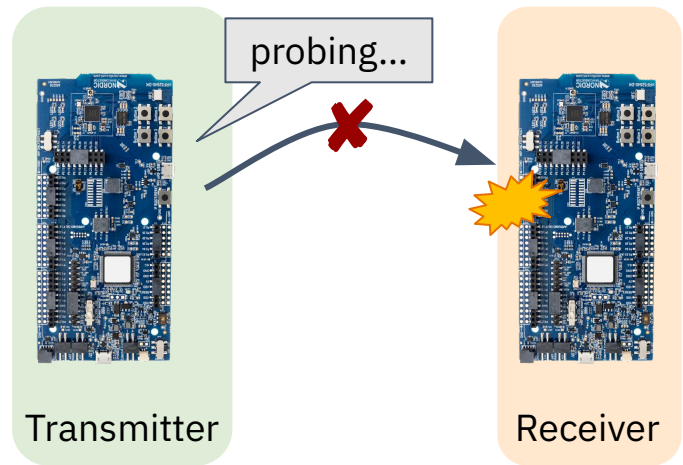
Reducing energy usage by filtering traffic

Invalid message causes receiver to respond.



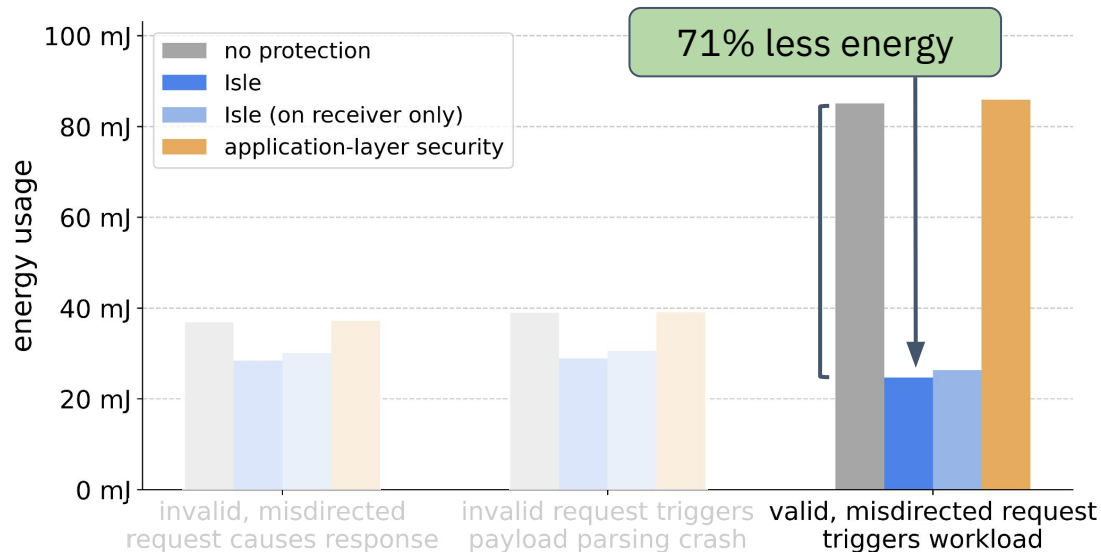
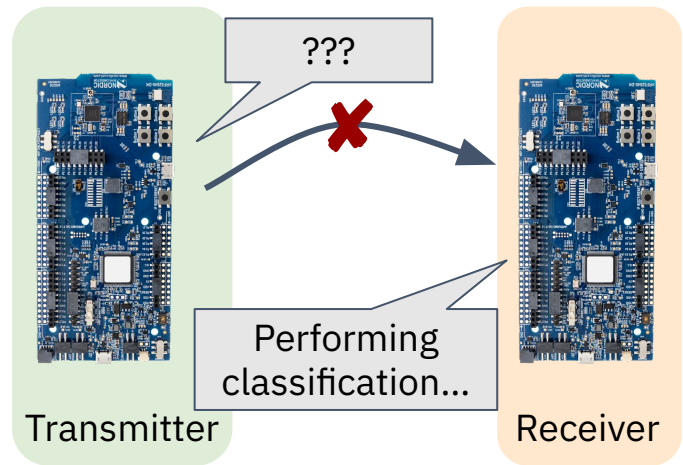
Reducing energy usage by filtering traffic

Invalid request causes receiver to crash.

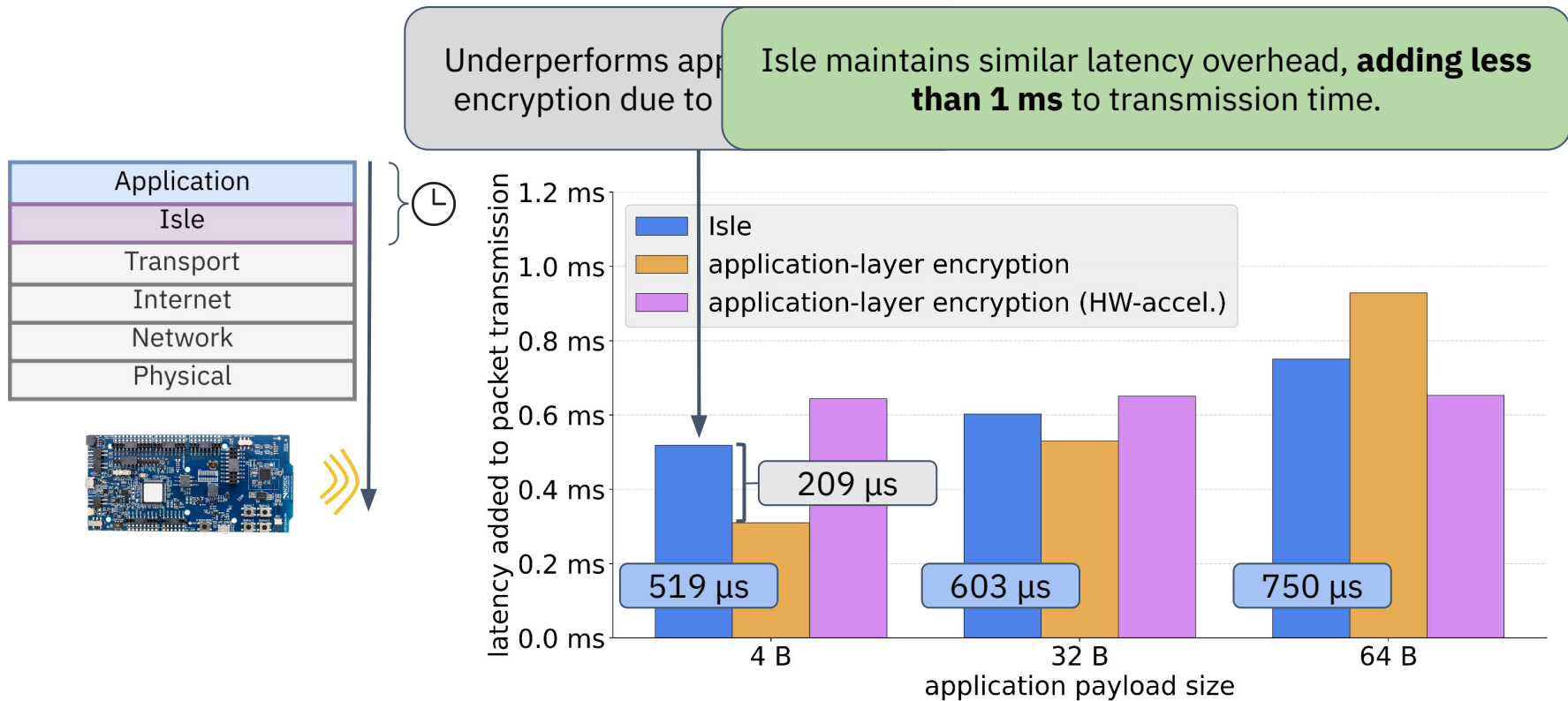


Reducing energy usage by filtering traffic

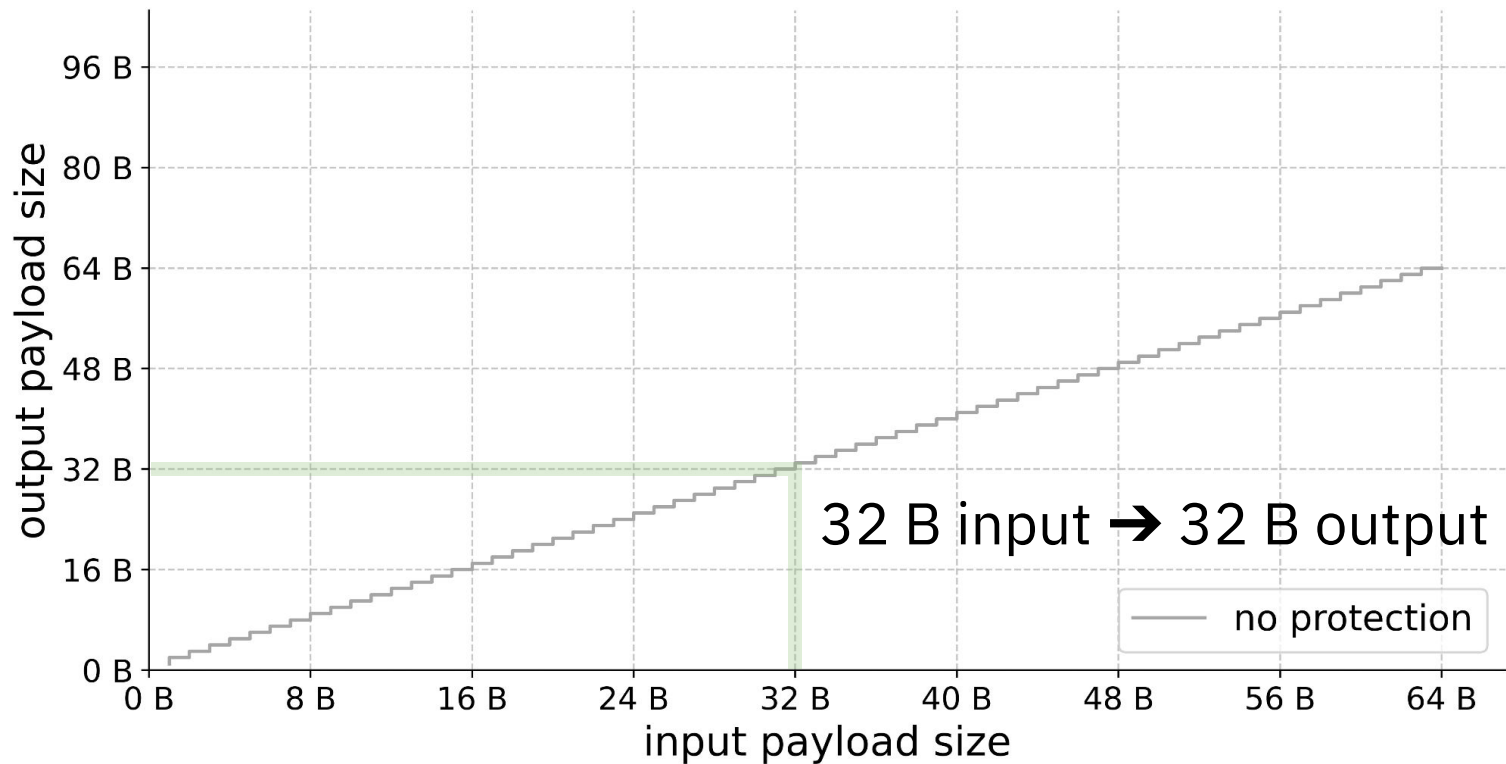
Misdirected request triggers workload.



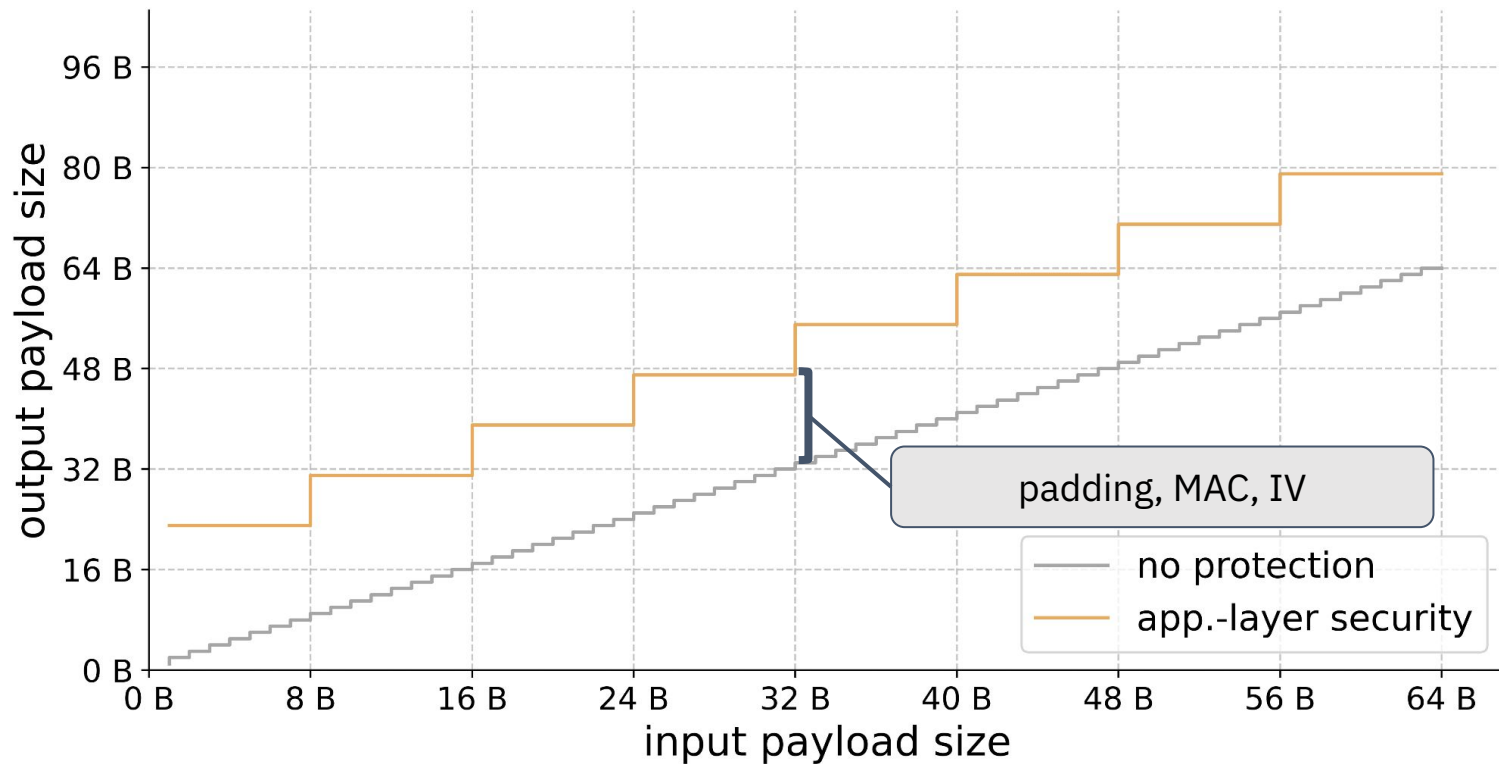
Additional latency for applying security



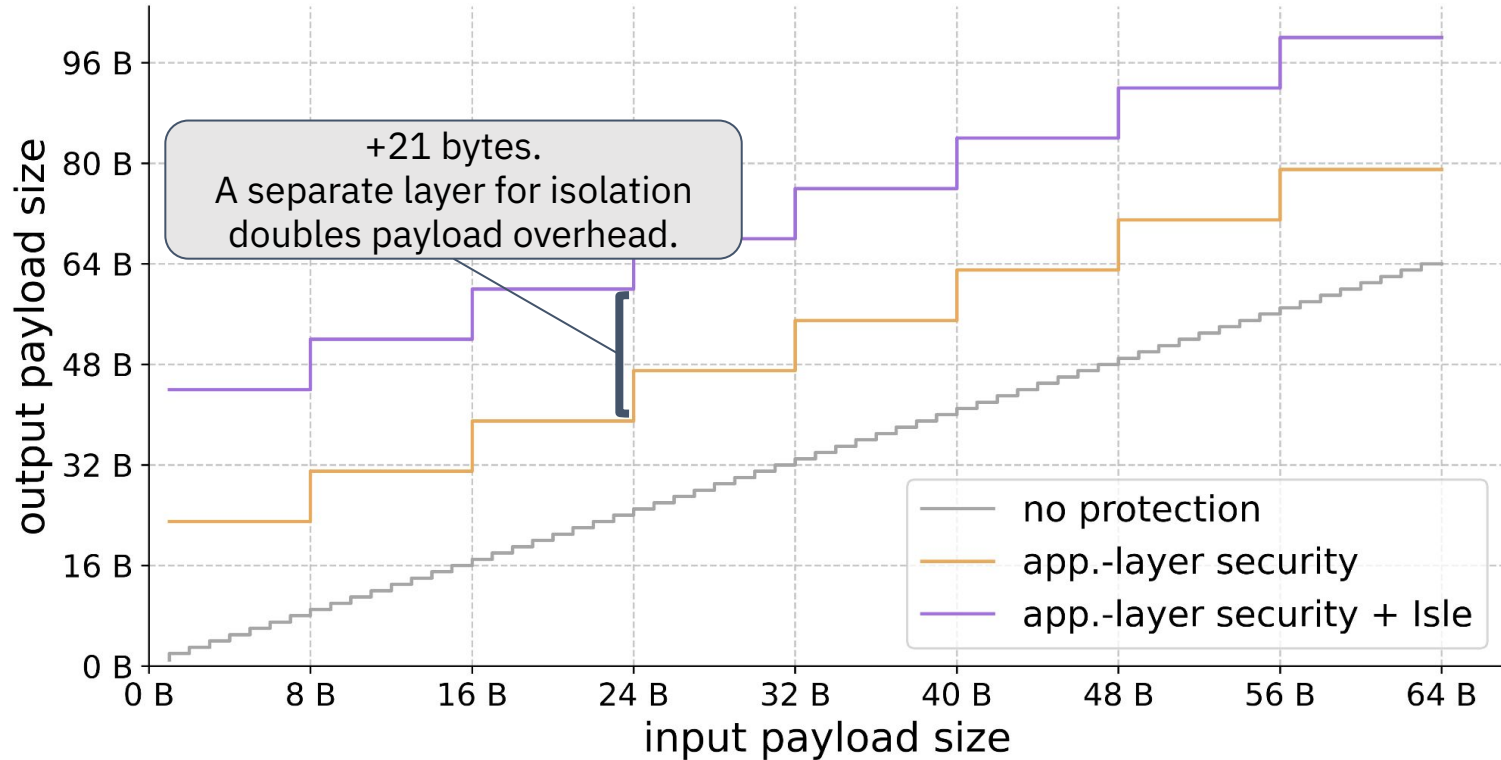
Additional packet data overhead



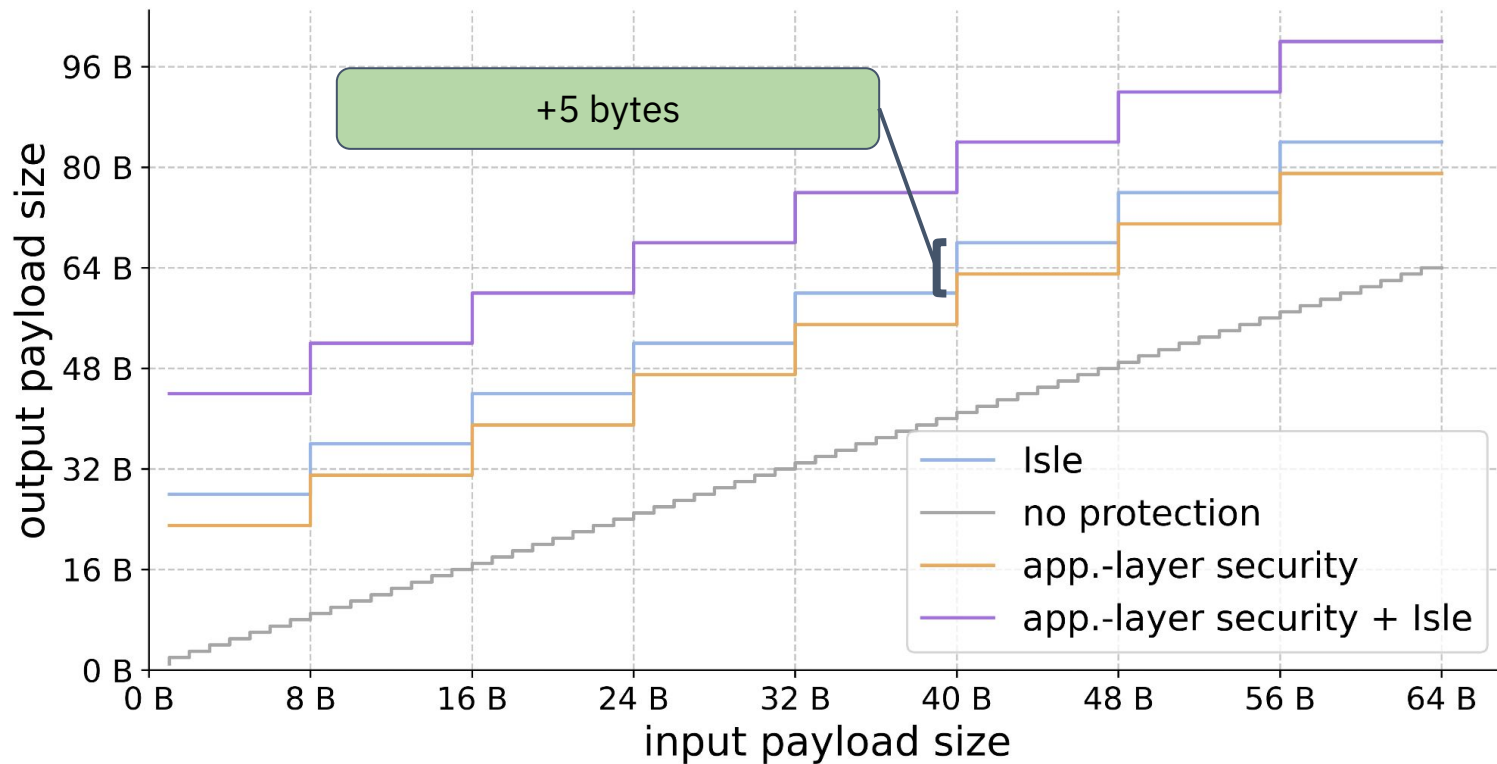
Additional packet data overhead



Additional packet data overhead



Additional packet data overhead



Conclusions

The trend toward unified mesh networking is a positive one but requires controls to keep the network efficient and suitable for embedded devices.

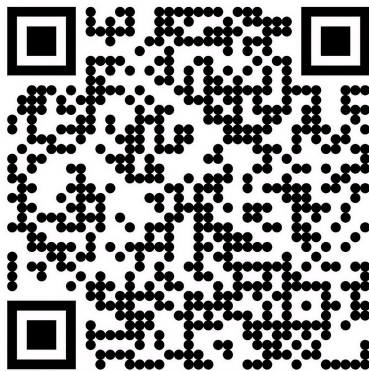
- **Isle offers control**, constraining applications **without impairing mesh structure**.
 - Re-use application-layer security to enforce isolation.
 - Provides control with sensitivity to overheads.
 - Conserves energy usage by blocking irrelevant traffic.

Thank You

Paper



Code



Marshall Clyburn



marshallc@virginia.edu



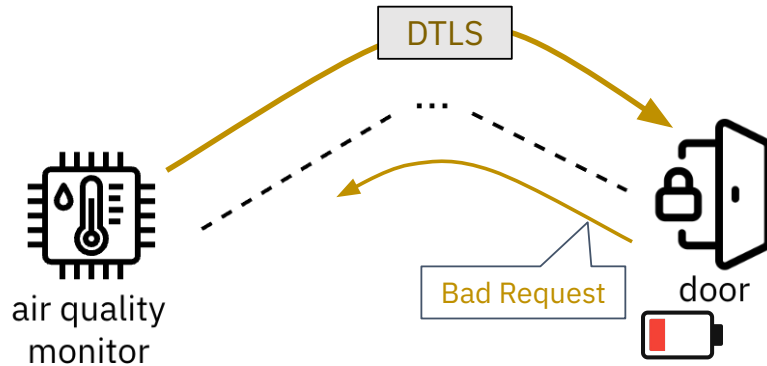
<https://mardev.net>



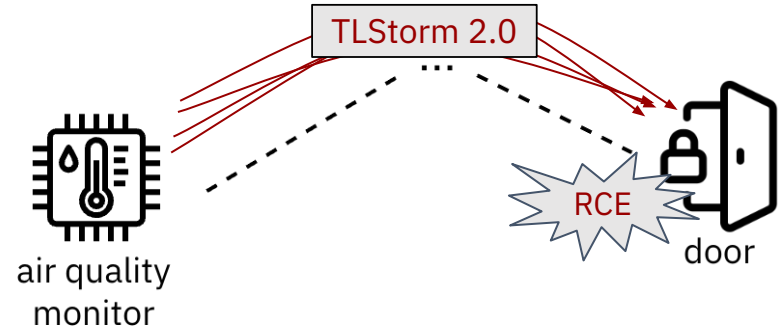
@mdclyburn

Additional Slides

Non-solutions for application isolation



Even a *correct* response wastes resources.

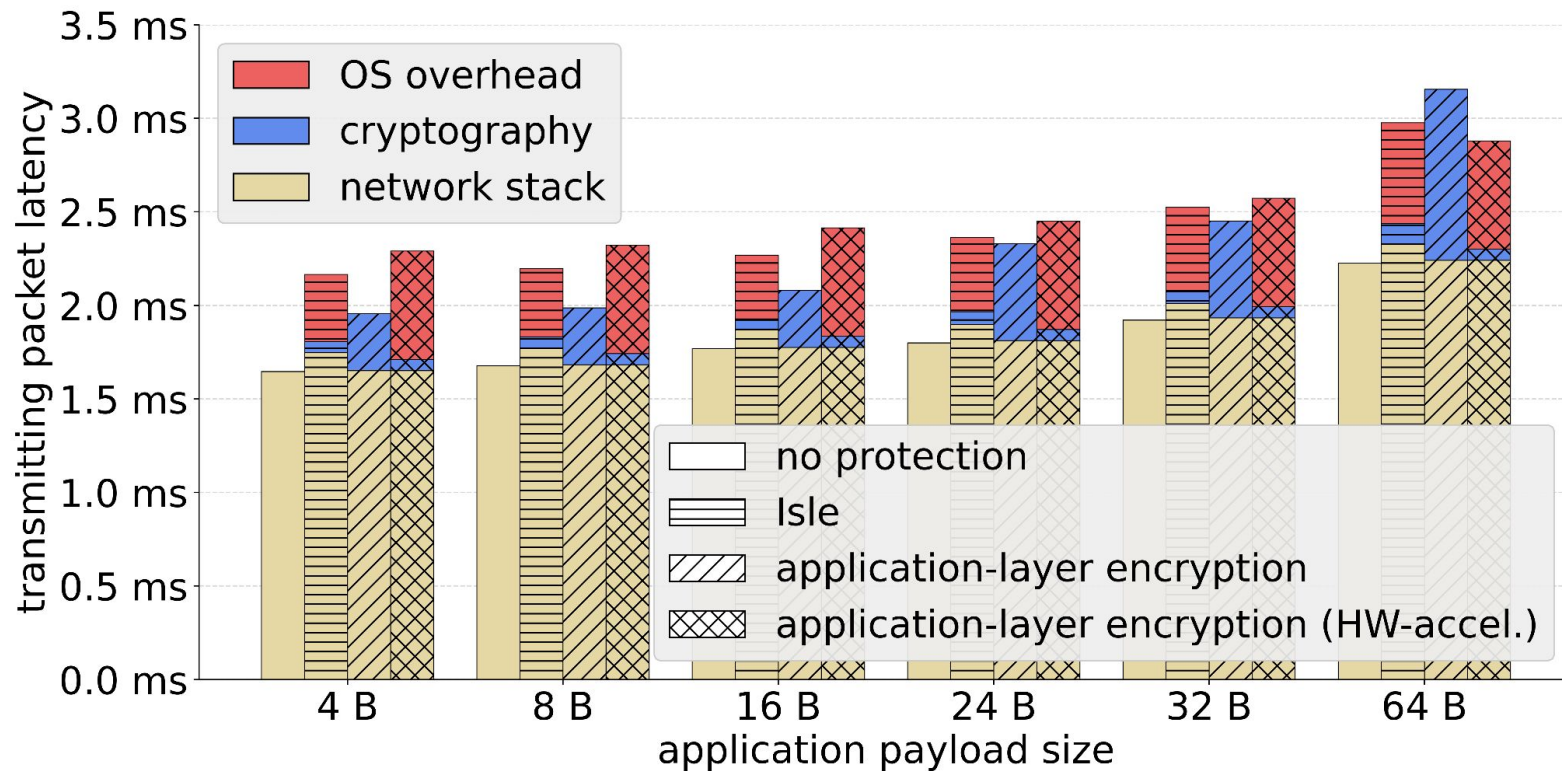


Implementation of (D)TLS may *itself* be vulnerable.

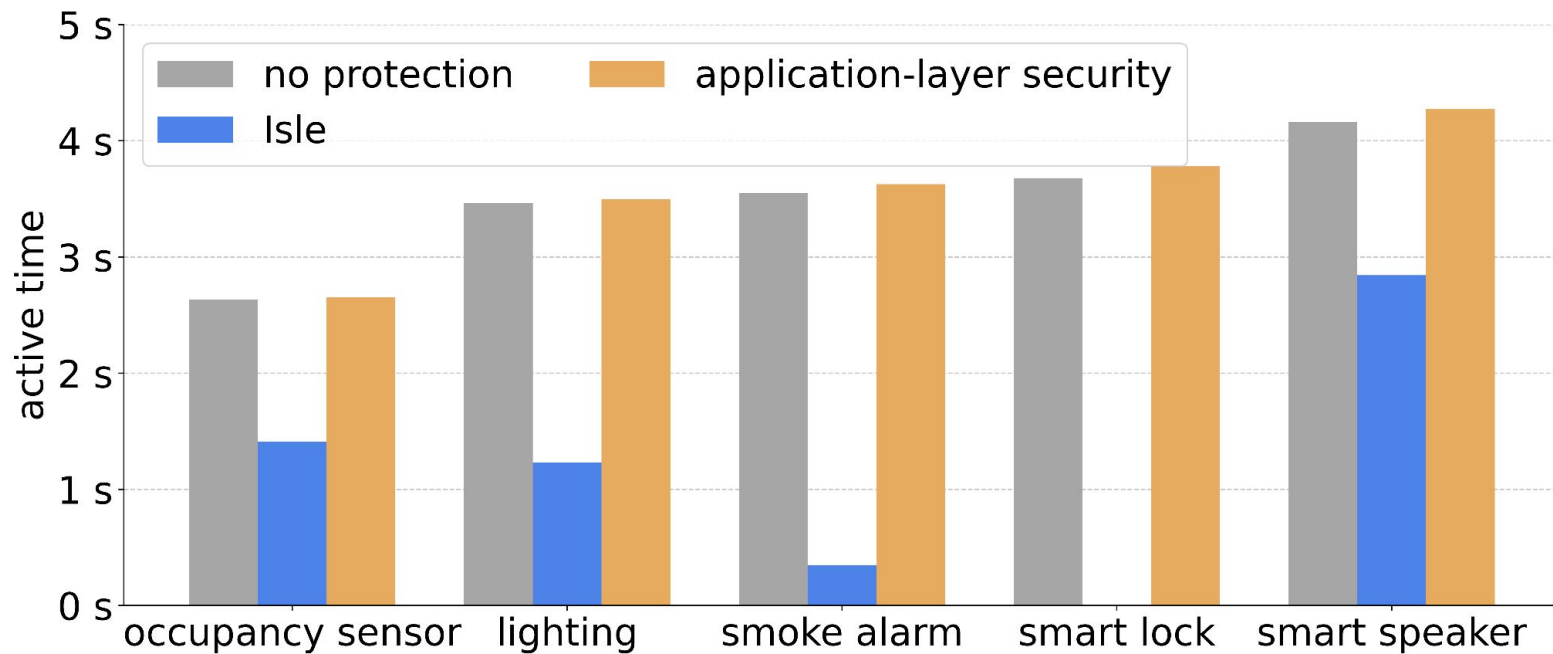
CVE-2024-45064

- STMicroelectronics' RTOS
- Web server application offering PUT can be exploited to achieve RCE.
- The application is vulnerable by receiving a particularly crafted sequence of packets.

Network TX overhead, profiled



Isle constrains aberrant traffic



Additional packet data overhead

