Toward Protecting Internet-Accessible Legacy Systems

Coauthors:

William Yurcik | Medicare HQ

Gregory Koenig | Independent Researcher

Gregory Pluta | University of Illinois at Urbana-Champaign

Gianni Pezzarossi | University of Illinois at Urbana-Champaign

Stuart Turner | University of Illinois @ Urbana-Champaign

Fabio Roberto de Miranda | Insper

Luciano Pereira Soares | Insper

The views expressed in this presentation are those of the authors alone and do not represent official positions or policy of their listed organizational affiliations to include the U.S. Federal Government.

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Legacy Systems

What are they? Outdated technologies still in active use.

The Problem: Cannot integrate with current technologies/functionality AND large structurally embedded security issue in critical sectors.

Key Driver: "Technical Obsolescence" – growing gap between a system's original design and its current use.

Why do organizations keep them?

- Stable, predictable, well-understood, & operational
- High replacement cost including transition risks
- Operational dependency

Characteristics of Legacy Systems

Beyond End-of-Life Support:

No more updates or maintenance from the vendor.

No Longer Available for Purchase:

Relies on obsolete technology.

Shrinking Workforce:

Requires developers with expertise in outdated languages.

High Maintenance:

Frequent and time-intensive repairs.

Vulnerability Exploitation:

Exposed to cybersecurity vulnerabilities without patches.

Case Study: Scientific Instruments

High-value, sensitive scientific instruments shared globally.

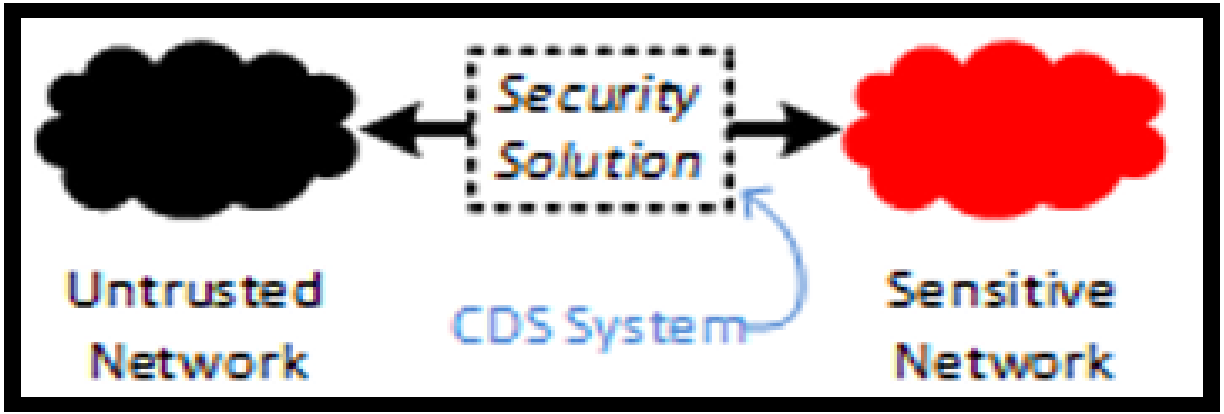
Key Challenges:

- Instruments outlast software/OS lifecycles.
  (20-30 years vs 2-8 years)
- Embedded software tied to outdated OS.
- Security patches and upgrades are difficult.

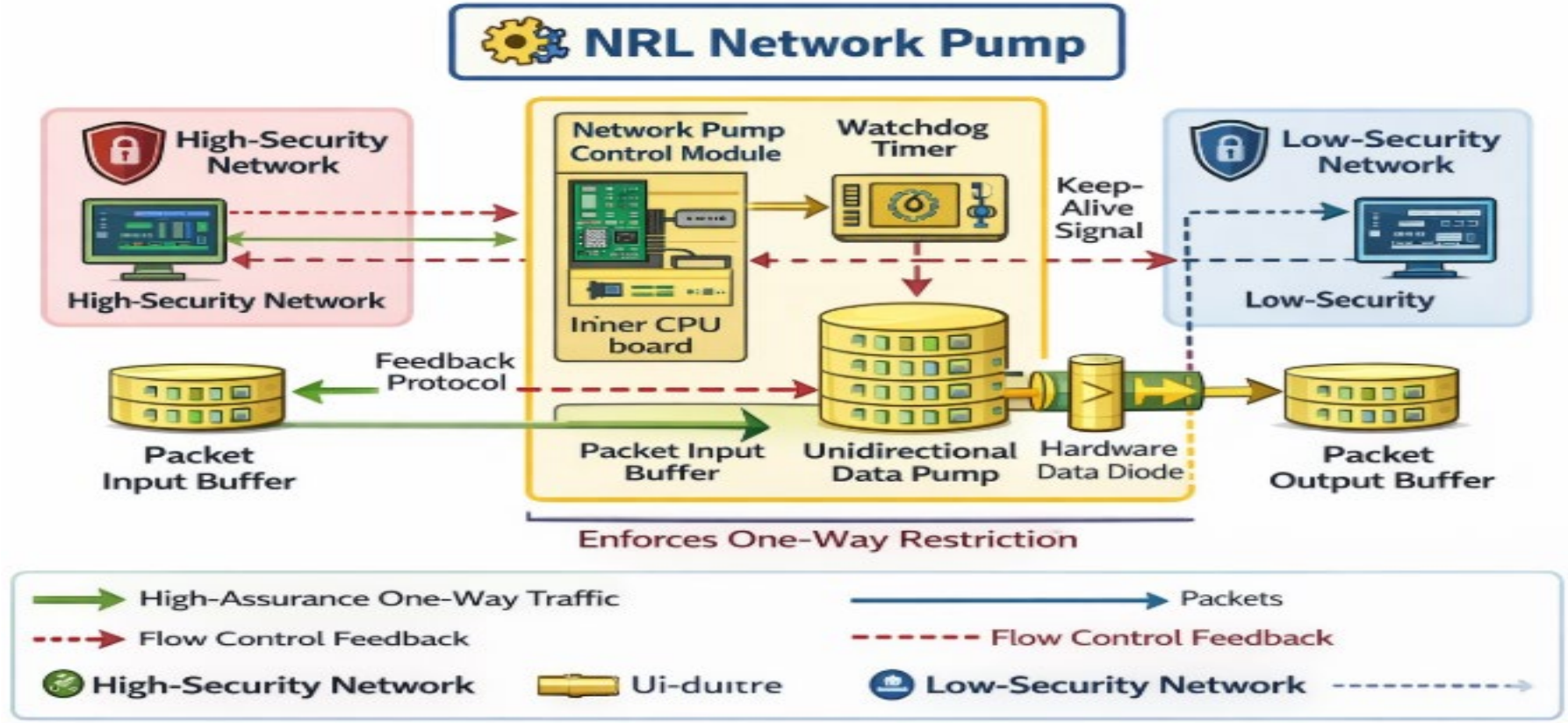
Potential Solutions

- Cross-Domain Solutions
- NRL Network Pump
- Network Data Diode
- Cloudlet Edge Computing

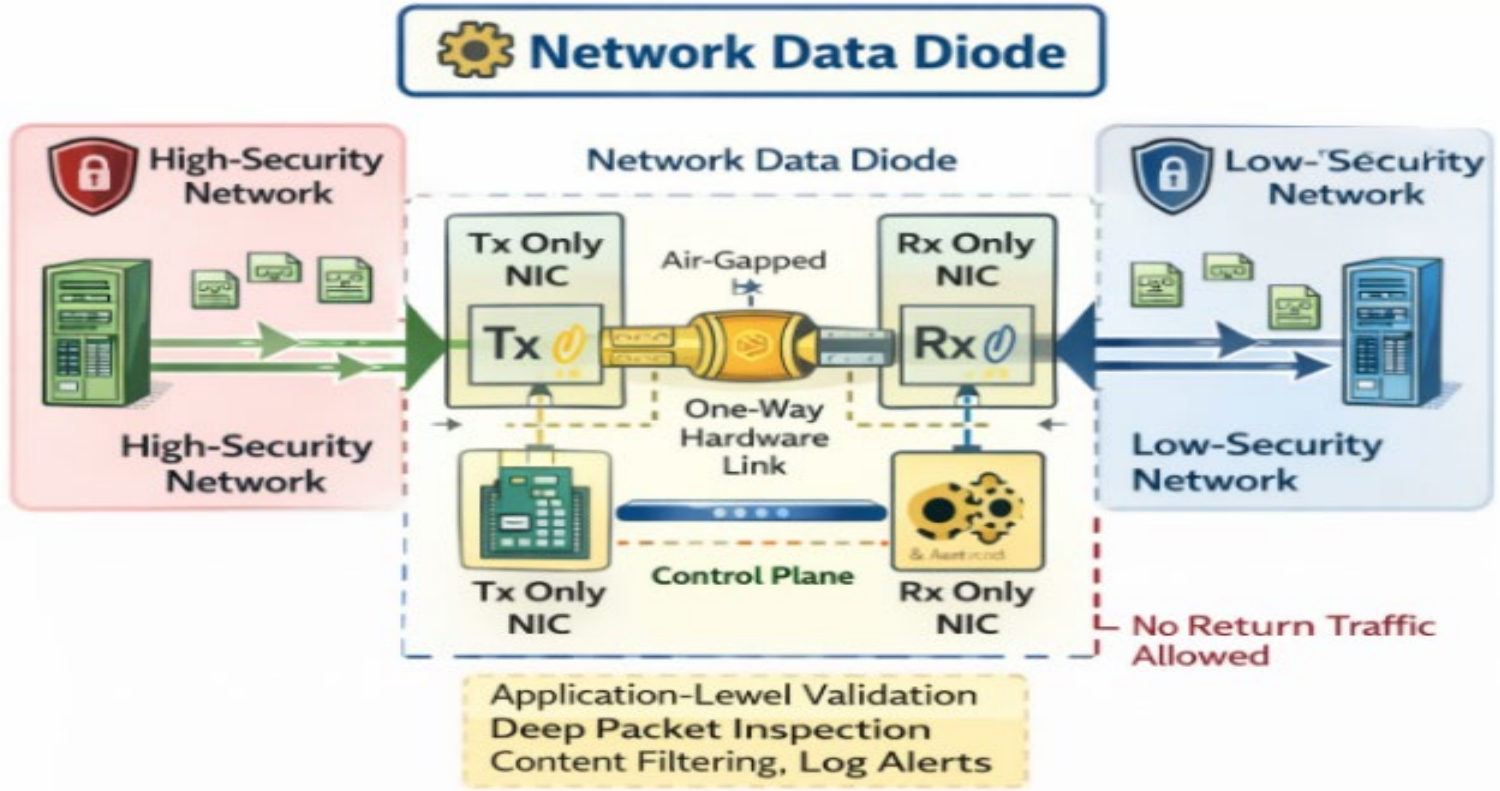
Cross-Domain Solutions



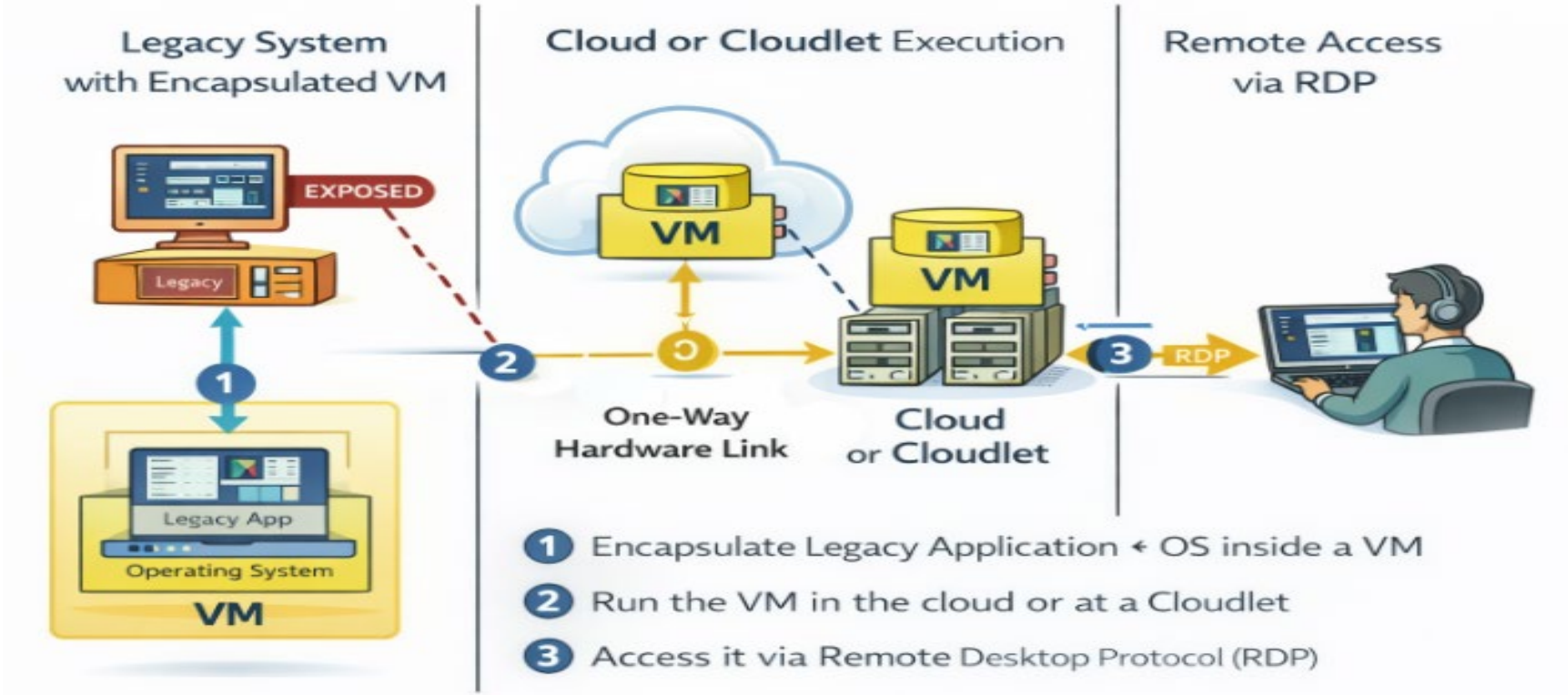
NRL Network Pump



Network Data Diode



Cloudlet Edge Computing



Conclusions & Future Work

The security problem with legacy systems is critical, widespread, and economically entrenched.

Potential Solutions Presented:

1. Controlled Sharing Between Trust Zones (Cross-Domain Solutions)
2. Highly-Controlled SW Mapping Data Transfer (NRL Network Pump)
3. Hardware One-Way Air Gap Data Transfer (Data Diodes)
4. Architectural Relocation of Systems to Virtual Cloudlets (EdgeVDI)

Future Work: Experiment, test, and share empirical research results for these potential solutions!