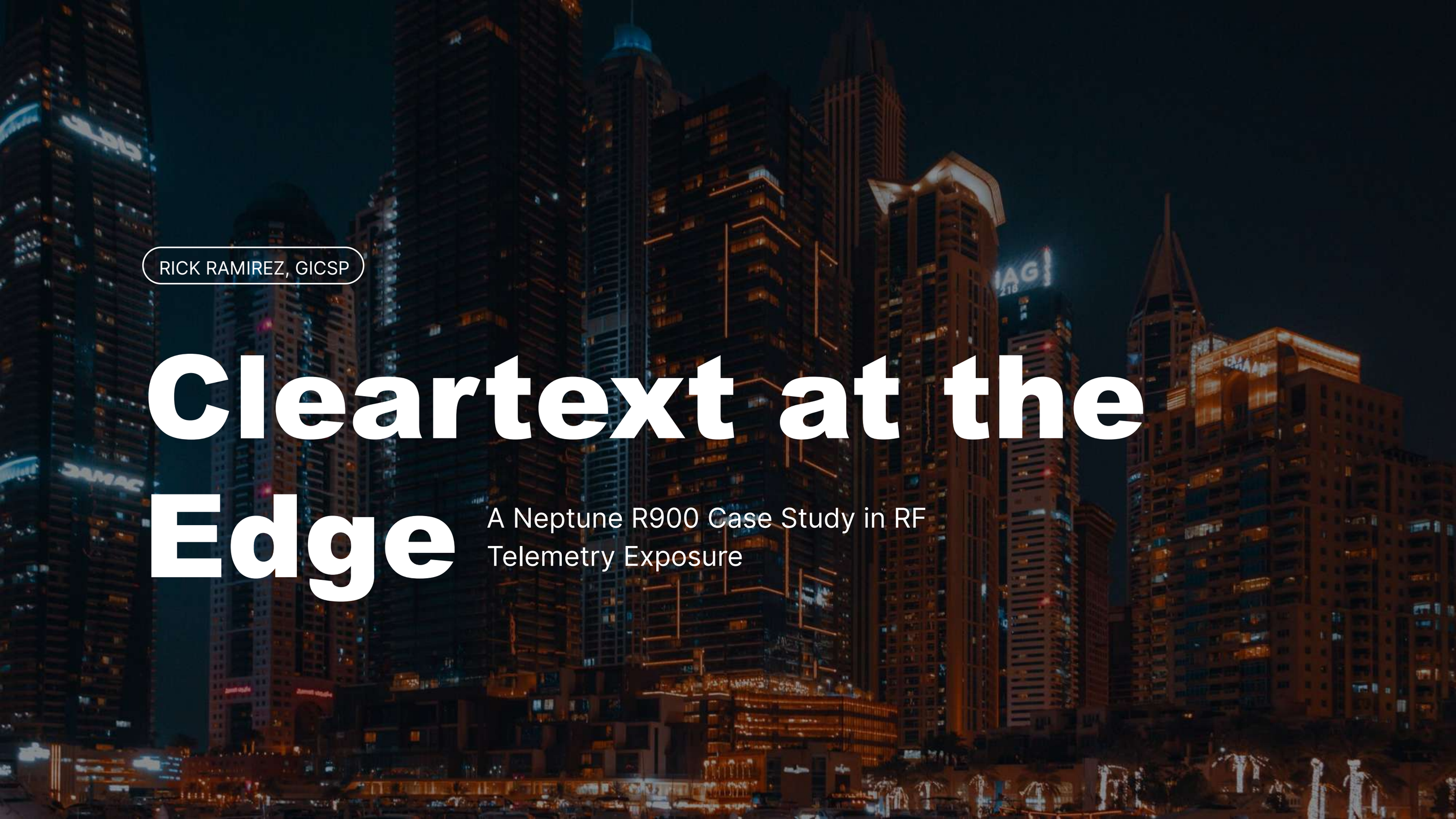


RICK RAMIREZ, GICSP

Cleartext at the Edge

A Neptune R900 Case Study in RF Telemetry Exposure

Whoami

- Rick Ramirez
- Lead Product Security Engineer
- OT/ICS, product security, medical device security, and cyber-physical systems
- Trained as a U.S. Marine Corps radio/electronics technician
- Research focus: passive RF telemetry, smart utility systems, and cyber-physical privacy risk

What This Talk Is and Is Not

THIS TALK IS:

- A passive RF case study
- A privacy and security analysis
- A discussion of systemic design risk
- A call to treat RF as part of the attack surface

THIS TALK IS NOT:

- A guide to targeting specific meters
- A release of raw sensitive telemetry
- An attempt to disrupt utility systems
- An exploitation walkthrough

Security Teams Know Networks. RF Is Often the Blind Spot.

- Security programs focus on endpoints, networks, cloud, identity, and applications
- Many cyber-physical systems communicate outside traditional network visibility
- RF traffic may never appear in firewall logs, EDR, SIEM, or packet captures
- If a system transmits, someone may be able to receive

“The boundary is not the firewall. The boundary is wherever the signal can be heard.”

RF Changes the Security Model

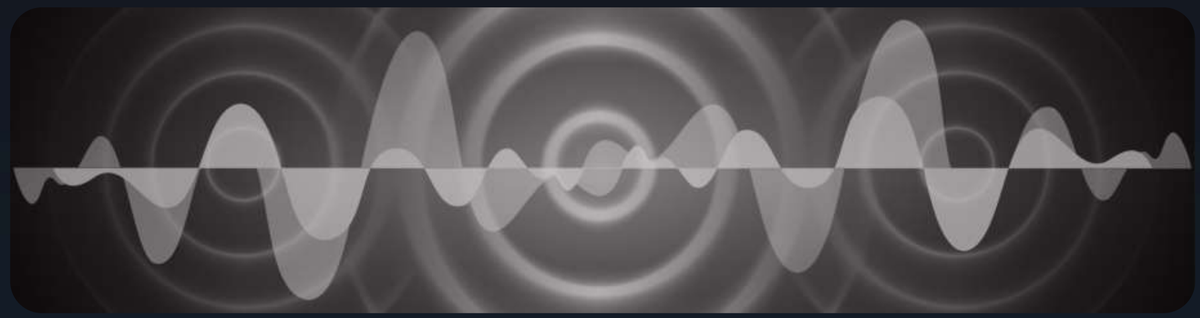
TRADITIONAL NETWORK SECURITY

- Requires network access
- Traffic is visible to network tools
- Boundaries are logical
- Packet capture starts at an interface
- Access often requires credentials

RF SECURITY

- Network Access may only need proximity
- Traffic visible through spectrum
- Boundaries are physical and environmental
- RF capture starts at the signal layer
- Access to data may only require an antenna

RF 101: Wireless Communication before the Packet



WHAT IS RF

- Radio Frequency is electromagnetic energy used to transmit information wirelessly.
- It is the physical medium behind many systems security teams already know.
- Examples: Wi-Fi, Bluetooth, cellular, key fobs, garage doors, LoRa, smart meters, and industrial telemetry.

DATA TRANSMISSION

- Devices transmit signals at specific frequencies.
- Data is placed onto the signal through modulation.
- A receiver captures the signal, demodulates it, and turns it into bits or protocol fields.

SECURE RF

- Encryption: protects the confidentiality of transmitted data
- Authentication: helps confirm the message came from a trusted device
- Rolling identifiers: reduce long-term tracking from static IDs
- Replay protection: prevents old messages from being reused as if they were new
- Signal/range management: limits unnecessary exposure where feasible

Software Defined Radios make RF Observable

- SDR allows a computer to receive and analyze RF signals
- One flexible receiver can observe many protocols and frequencies
- Low-cost SDR devices make RF research more accessible
- Tooling used in this research: RTL-SDR, antenna, rtl_433, GNU Radio optionally for deeper analysis, and long-duration captures

902 - 928 MHz the ISM Band

- Unlicensed ISM band in the United States
- Used by many low-power devices
- Common in utility, industrial, and consumer telemetry
- Better range and penetration than many higher-frequency systems
- Co-resident technologies can include:
  - Smart utility meters
  - LoRa devices
  - Wireless sensors
  - Alarm systems
  - Consumer IoT

Radio Frequency Spectrum

Source: Roufa et al.

From Radio Signals to Data

RF waveform / Baseband signal

Recovered symbols

Digital livestream

Parsed packets & structures

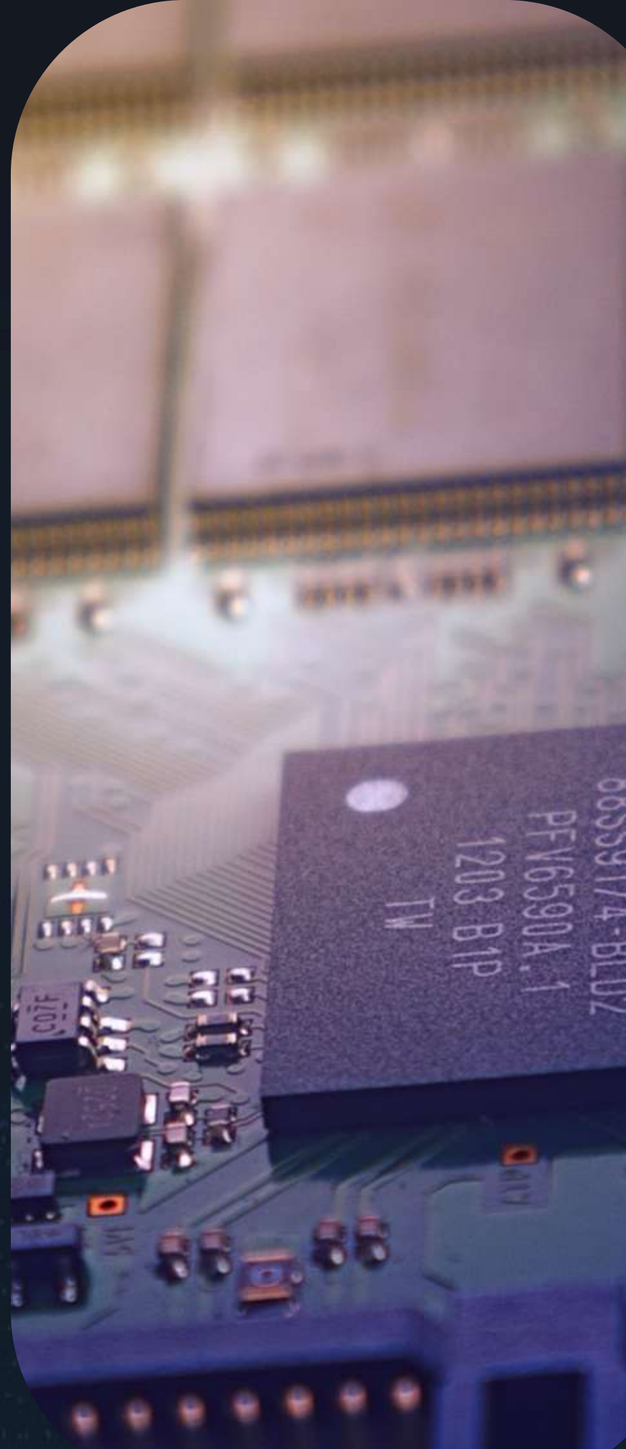
Extracted data points

Methodology: Passive Receive-Only Observation

- Identify RF activity in the 902-928 MHz band
- Use SDR tooling to observe transmissions
- Decode supported telemetry protocols
- Log repeated observations over time
- Sanitize data for analysis
- Assess security and privacy implications

RESEARCH BOUNDARIES

- No transmission
- No disruption
- No meter interaction
- No raw sensitive data shared
- Data minimization and sanitization
- Observation of my own home data only



Case Study: Neptune R900i

DEVICE OVERVIEW

- AMR Endpoint / Transmitter
- 902-928 MHz ISM Band
- No Encryption, No Authentication
- Millions of units across North American water utilities

KEY FINDINGS

- Transmits real-time water usage, meter ID, and status in cleartext
- Remotely readable with < $100 SDR hardware using passive reception
- Enables customer surveillance, occupancy inference, and pattern analysis
- No cryptographic protections of transmitted data

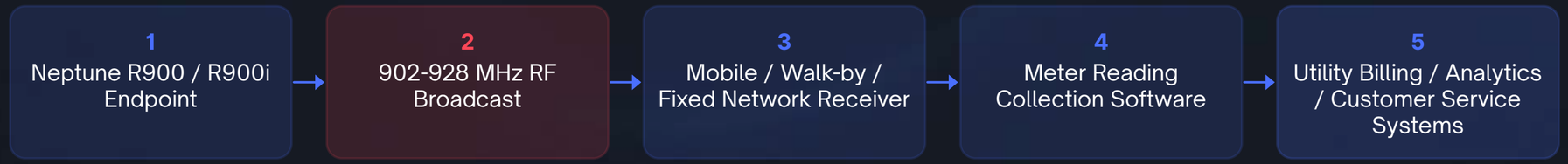
IMPACT

Mass surveillance of water usage, privacy violations, and critical infrastructure risk due to systemic unencrypted telemetry.

Capture Setup

Neptune R900i	Cleartext Signal	RTL-SDR Receiver	RTL_433 Decoding Tool	Telemetry Data

AMR Data Flow: From Meter to Utility Systems



⚠ **SECURITY CONCERN**

The RF segment is outside traditional network visibility and may expose cleartext telemetry before it reaches utility-controlled systems.

What a Decoded Frame Can Reveal

Example JSON Output:

```
{
"model": "Neptune-R900",
"id": "Unique Meter ID",
"consumption": “Water Usage Amount”,
"leak": 0,
"backflow": 0,
"rssi": "Signal Strength",
"time": "Time signal was transmitted"
}
```

- Protocol/model
- Meter ID
- Consumption reading
- Leak indicator
- Backflow/tamper-style status fields, where present
- Signal strength
- Timestamp

Live Demo

Passive RF to Structured Telemetry

```
switching to live terminal...
```

Telemetry Can Become Pattern of Life Data

DAILY ROUTINES

Consumption Telemetry can potentially reveal occupancy patterns and give observers insight on your daily life.

INDUSTRIAL ENVIRONMENTS

Consumption of water can give insight to manufacturing, water treatment or other sensitive and critical processes.

VACANT AND AWAY PERIODS

Understanding daily usage patterns gives insights on when the likelihood of vacancy of a building is higher.

Risk Rating Methodology

METHOD USED:

A qualitative Likelihood × Impact risk model, with a privacy and cyber-physical context overlay.

DIMENSION	MEASUREMENT	RATING FACTORS
Likelihood	How feasible the threat event is	Required access, cost, skill, proximity, tooling availability
Impact	What exposure or harm could result	Confidentiality loss, privacy inference, operational visibility, trust boundary weakness
Context	Why this matters beyond a single packet	Critical infrastructure sector, deployment scale, persistence, aggregation, lack of user visibility

LIKELIHOOD - HIGH

- Passive receive-only
- No authentication required
- Low-cost SDR tooling
- No user interaction
- RF proximity-based

IMPACT - HIGH

- Persistent identifiers
- Consumption telemetry
- Status flags
- Potential pattern-of-life inference
- Asset enumeration

CONTEXT - HIGH

- Water and wastewater critical infrastructure
- Long device lifecycle
- Public RF propagation
- Limited customer visibility
- Scales across neighborhoods and municipalities

Security & Privacy Risks

	RISK	WHY IT MATTERS	RISK DRIVER	RISK RATING	RECOMMENDATION
	Passive Surveillance	No interaction with target required	Low cost receive only collection	High	Encrypt telemetry in future deployments
	Static Identifiers	Enables long term tracking	Persistent device identity	High	Use rotating or pseudonymous identifiers
	Cleartext Telemetry	Data readable by unintended receivers	No encryption or access control	High	Treat RF range as a trust boundary
	Pattern of life inference	Usage can reveal behavior	Repeated time series data	High	Minimize broadcast frequency and exposed fields
	Asset enumeration	Devices can be discovered at scale	Neighborhood level RF observability	Medium - High	Authenticate telemetry before downstream trust
	Weak Trust Boundaries	Operational data leaves controlled environments	Broadcast beyond intended receiver	High	Add RF security review to procurement
	Integrity Concerns	Unauthenticated telemetry may create replay/spoofing concerns.	No message authentication	Medium - High	Plan phased replacement for legacy endpoints

So What? Why This Matters

This is not just a meter issue. It is a visibility, privacy, and trust-boundary issue for cyber-physical systems.

For Residents

- Water usage can reveal patterns of life
- Static IDs can enable long-term tracking
- Exposure happens without customer awareness

For Utilities

- RF telemetry becomes part of the attack surface
- Legacy AMR design choices create modern privacy risk
- Procurement decisions can lock in exposure for years

For Security Teams

- RF signals may bypass normal security tooling
- The system boundary extends beyond the firewall
- Passive telemetry should be included in threat modeling

⚠ If a critical system transmits beyond the controlled environment, that signal path deserves the same security scrutiny as any network connection.

Disclosure Scope Beyond the Case Study

This talk focuses on Neptune Technology Group R900 as the primary case study:

- CISA disclosure process February 2026 closed May 2026
- During CISA disclosure process attempts to communicate with Neptune Technology.
- Neptune Technology has yet to respond to communication attempts.

The broader disclosure included observations involving multiple AMR/AMI vendors:

- Itron (Gas, Electric)
- Neptune Technology Group (Water, Sewer)
- Badger Meter (Water, Sewer)
- Landis+Gyr (Electric)

During the CISA-coordinated disclosure process, **I did not receive direct responses from most vendors**
Landis+Gyr was the exception and provided a Customer Information Letter (CIL) to impacted customers.

This Is Bigger Than One Meter

- Neptune R900 is the case study, not the entire problem space
- Cleartext or weakly protected RF telemetry appears across multiple utility telemetry ecosystems
- The issue is systemic:
  - Legacy design assumptions
  - Long device lifecycles
  - Public RF propagation
  - Limited customer visibility
  - Utility procurement dependencies
- Security teams need to evaluate RF telemetry as a class of exposure

What Security Teams Should Take Away

DESIGN CONTROLS

- Encrypt sensitive telemetry payloads
- Authenticate messages
- Add replay protection
- Avoid static identifiers where possible
- Reduce unnecessary broadcast fields

PROGRAM & PROCUREMENT CONTROLS

- Treat RF telemetry as an external-facing interface
- Include RF in threat modeling and architecture reviews
- Add RF security requirements to procurement language
- Conduct privacy impact assessments for AMR/AMI deployments
- Monitor for abnormal RF behavior where feasible

KEY TAKEAWAYS

- RF is part of the attack surface.
- Passive observation can reveal structured telemetry
- Cleartext data creates risk when repeated over time
- Cyber-physical privacy requires thinking beyond the network
- Security reviews should include the signal layer

Thank You

Questions & Discussion

Signal layer security starts with visibility.

CONTACT

rramir.securityresearch@protonmail.com

www.linkedin.com/in/rickramir