

Securing Critical Infrastructure

1. Executive Summary

In an era of geometric increases in number and type of cyber threats to critical infrastructure, permanent connections to external networks elevate the risk of successful attacks. This white paper introduces a revolutionary approach to protecting vital systems by keeping them offline and allowing external access only when necessary.

A comprehensive “off-grid by default” approach (in conjunction with existing measures) represents a paradigm shift in infrastructure security, offering unparalleled protection against cyber-attacks while maintaining operational efficiency. This approach has the added benefit of providing a robust, dynamic authentication system for remote access.

2. Introduction

Critical infrastructure – including power grids, water treatment facilities, industrial control systems, and transportation networks – forms the backbone of modern society. As these systems become increasingly interconnected and reliant on internet-based communications, they also become more vulnerable to

cyber-attacks. Traditional security measures, while necessary, often struggle to keep pace with evolving threats.

The limitations of always-on security approaches are becoming increasingly apparent. Constant connectivity, while operationally convenient, provides attackers with a persistent target. Even the most robust firewalls and intrusion detection systems can be compromised given enough time and resources. Moreover, the rise of remote work has introduced new vulnerabilities in accessing these critical systems.

This white paper presents a novel solution that fundamentally alters the security paradigm for critical infrastructure. By integrating a Software Defined Mobile Network Operator (SD-MNO) technology into the network operation, we can create a dynamic, controlled connectivity environment that dramatically reduces exposure to internet-based threats and provides secure, authenticated remote access.

3. Technology Overview

The core of this solution is based on SD-MNO technology, originally developed as a dynamic authentication solution to secure communications. This technology allows for the creation of a virtual, on-premises Mobile Network Operator (MNO) that can dynamically provision and manage connectivity, identities, and routing through software control, akin in some respects to how Software Defined Networking (SDN) has revolutionized network management.

Key features of the SD-MNO technology include:

- Dynamic IMSI (International Mobile Subscriber Identity) rotation
- IMEI (International Mobile Equipment Identity) management
- Custom routing controls
- On-demand connectivity provisioning
- Secure authentication for remote access

By integrating this technology with standard routers, gateways, and firewalls used in critical infrastructure, we can extend these powerful security features to vital systems, creating a new layer of protection against cyber threats and ensuring secure remote access.

4. The Concept: Controlled Connectivity and Dynamic Authentication

The fundamental principle behind this approach is “off-grid by default.” Instead of maintaining constant internet connectivity, critical systems remain isolated from the broader internet except when necessary. This approach dramatically reduces the attack surface available to potential threats. And when systems come online they never connect to the broader Internet through the same paths.

Key aspects of the controlled connectivity concept include:

- Default Isolation: Systems remain disconnected from the internet by default.
- On-Demand Connectivity: Internet access is provisioned only when required for specific opera-

tions, updates, or monitoring.

- **Rapid Disconnect:** Systems can quickly terminate internet connections once tasks are completed.
- **Dynamic Identity:** When online, systems use rotating identifiers to prevent tracking and targeted attacks.
- **Secure Remote Authentication:** Authorized personnel use specially equipped User Equipment (UE) for multi-factor, dynamic authentication.

By implementing this approach, we create a moving target that is incredibly difficult for attackers to pin down or exploit, while ensuring that only authorized personnel can access critical systems remotely.

5. How It Works

The integration of SD-MNO technology with critical infrastructure routers/gateways/firewalls involves both hardware and software components:

Hardware Integration:

- A specialized module (or external device) is added to existing network equipment.
- This module contains SIM capabilities and interfaces with the SD-MNO system.
- Authorized remote workers are equipped with UEs (User Equipment) that utilize the same IMSI rotation technology.

Software Control Mechanisms:

- A secure, on-premises control system¹ manages connectivity and authentication.
- Administrators can set policies for when and how systems connect to the internet and who can access them remotely (automated or ad hoc).
- Automated systems can request temporary connectivity when needed.

Connectivity and Authentication Protocols:

- When internet access is required, the system provisions a connection using a randomly selected IMSI.
- Connections are time-limited and automatically terminate once tasks are completed.
- For remote access, the worker's UE provides a dynamic, rotating IMSI that serves as an additional authentication factor.
- The infrastructure verifies both traditional credentials and the UE's current IMSI before granting access.

1. An autonomous SD-MNO cloud is deployed internally in customer's environment e.g. AWS

6. Key Benefits

This approach offers several significant advantages over traditional always-on security:

- **Dramatically Reduced Exposure:** By minimizing the time systems are connected to the internet, we significantly reduce the window of opportunity for attackers.
- **Enhanced Control:** Administrators have granular control over when and how systems connect to the internet and who can access them.
- **Improved Monitoring:** All connectivity and access events are logged, providing a clear audit trail.
- **Moving Target Defense:** Dynamic identifiers make it extremely difficult for attackers to track or target specific systems.
- **Multi-Factor, Dynamic Authentication:** Remote access is secured through both traditional credentials and time-sensitive, rotating UE identifiers.
- **Layered Security:** This approach complements existing security measures, adding multiple layers of protection.

7. Use Cases

This technology can be applied across various critical infrastructure sectors:

Power Grid Infrastructure:

- Control systems connect only for essential updates or remote monitoring.
- Grid management software uses brief, secure dynamic IMSI authenticated connections for data exchange.
- Remote technicians use UE-based authentication for emergency access.

Water Treatment Facilities:

- Monitoring systems connect periodically to report status.
- Remote access for maintenance is provided through time-limited, secure dynamic IMSI authenticated connections with UE authentication.
- **Industrial Control Systems:**
- Systems remain isolated during normal operations.
- Temporary connections allow for software updates and remote diagnostics, with strict dynamic IMSI authentication protocols.

Transportation Systems:

- Traffic management systems use brief, secure dynamic IMSI authenticated connections for data updates.

- Maintenance and monitoring systems connect on-demand, minimizing exposure.
- Remote access for emergency adjustments uses multi-factor, dynamic IMSI authentication.

8. Implementation Considerations

Integrating this technology into existing critical infrastructure requires planning:

- **System Assessment:** Evaluate current systems to identify connectivity requirements and remote access needs.
- **Gradual Integration:** Implement the technology in phases, starting with less critical systems.
- **Training:** Educate staff on new protocols, the importance of controlled connectivity, and proper use of UE for authentication.
- **Emergency Protocols:** Develop clear procedures for situations requiring immediate connectivity or remote access.
- **Failsafes:** Implement backup communication methods for critical alerts and notifications.
- **UE Management:** Establish protocols for securely distributing, managing, and revoking UEs for authorized personnel.

9. Security Analysis

Compared to traditional always-on approaches, this controlled connectivity and dynamic authentication strategy offers significant security advantages:

- **Reduced Attack Surface:** Minimal online presence gives attackers fewer opportunities to breach systems.
- **Dynamic Defense:** Rotating identifiers and connections prevent sustained attacks and credential theft.
- **Improved Incident Response:** Clear logs of all connectivity and access events aid in forensic analysis if a breach occurs.
- **Enhanced Remote Access Security:** Multi-factor, dynamic authentication significantly reduces the risk of unauthorized access.

10. Conclusion

The integration of Software Defined MNO technology with critical infrastructure routers, coupled with UE-based dynamic IMSI authentication for remote access, represents a paradigm shift in cybersecurity for vital systems. By implementing controlled connectivity and advanced authentication, we can dramatically reduce the exposure of critical infrastructure to internet-based threats while maintaining operational efficiency and ensuring secure remote access. This approach provides a powerful new tool in the ongoing battle to protect the systems that underpin modern society.

Protecting critical infrastructure requires innovative solutions that go beyond traditional security mea-

tures. We invite infrastructure operators, security professionals, and policymakers to explore how this controlled connectivity and dynamic authentication approach can enhance the security of vital systems. Contact us to learn more about implementing this Software Defined MNO technology and taking the next step in comprehensive critical infrastructure protection.