5G Network Slicing – C-SCRM Best Practices

“Thin-Crust” Recipe for Supply Chain Resilience

What is Network Slicing?

Network slicing is a network architecture that allows logical networks to share the same physical network infrastructure. Network slicing enables network providers to maximize use of a common infrastructure to deliver optimized services and applications isolated for multiple users. Fifth-generation (5G) technology standards for broadband cellular networks identify network slicing as a critical component.

A recent report by the Enduring Security Framework, “Potential Threats to 5G Network Slicing” (2022), further expounds:

> *A network slice is an end-to-end logical network that provides specific network capabilities and characteristics to fit a user’s needs. Although multiple network slices run on a single physical network, network slice users are authenticated for only one network area, enabling data and security isolation.*

Dedicated network slice use cases include:

- A mobile holographic or augmented reality system relying upon a 5G mobile broadband network with high bandwidth capacities for fast data and video streaming (capacity).
- Autonomous vehicle management requires high reliability and minimal latency in order to safely operate in dynamically changing environments (real-time performance).

5G Network Slicing Cyber Supply Chain (C-SCRM) Considerations

Network slicing maximizes shared network resources and service flexibility. It also enhances security through isolation and segmentation, thereby limiting the damage individual attacks can produce against a network. If an attacker hacks into one slice of the network, the other slices are isolated in a manner that will prevent the attacker from moving laterally across the network.

However, increased segmentation also results in a greater number of network slices for carriers to continuously manage and monitor to preserve network integrity and availability. Moreover, centralized network aspects such as certain control, management, or orchestration systems are attractive supply chain targets because these systems must connect to all slices of the network.

Slicing technologies, whether deployed in 5G, Ethernet, or software defined networks, are an attractive option for performance and security risk management. Because 5G Cyber Supply Chain Risk Management (C-SCRM) recommendations are extensible to other network domains, businesses can achieve broader returns on security investments by adopting these standards and best practices.

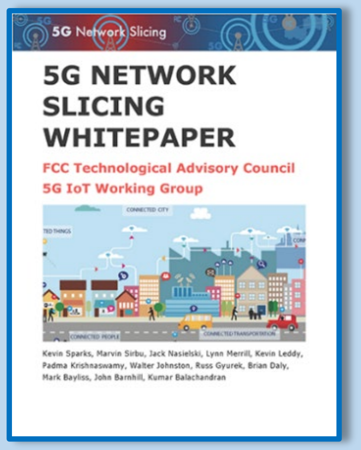
Network Slicing C-SCRM Recommendations

- Adopt Zero Trust Architecture to reduce the effectiveness of man-in-the-middle and configuration attacks and to protect the confidentiality and integrity of systems by continuously validating every stage of a digital interaction through strong authentication and authorization methods.
- Adopt Multi-Layered Security to prevent users from obtaining access to unauthorized information.
- Use Cross-Domain Solutions to enforce security policies and control the flow of information between interconnected information systems.
- Use Post-Quantum Cryptography algorithms once they are available and standardized for data protection and to mitigate potential future risks.

5G Network Slicing References

ESF Potential Threats to 5G Network Slicing

Enduring Security Framework: “Potential Threats to 5G Network Slicing” (2022)



5G Network Slicing

5G NETWORK SLICING WHITEPAPER

FCC Technological Advisory Council

5G IoT Working Group

Kevin Sparks, Marvin Sirbu, Jack Nasielski, Lynn Merrill, Kevin Leddy, Padma Krishnaswamy, Walter Johnston, Russ Gyurek, Brian Daly, Mark Bayliss, John Barnhill, Kumar Balachandran

FCC Technological Advisory Council: “5G Network Slicing Whitepaper” (2018)

Dated: 21 April 2023