Realizing a zero-trust architecture for 5G networks

Quick take

Alan McBride and Gaurav Kumar Agarwal

In this article, we discuss the relevance of the zero-trust concept to 5G. Robust access management is a foundational aspect of cybersecurity in general. It is required to protect all three primary security attributes: confidentiality, integrity and availability. Zero-trust is considered to be the current best practice in access management. It is a significantly more mature level of access management than traditional approaches that focus on perimeter security and password-based authentication. Unlike them it does not grant trust implicitly or by default, and it offers more optimal levels of granularity, flexibility and monitoring.

5G security challenges

5G is designed to serve a wide range of use cases through improved performance, reliability and latency. Notably, 5G's network slicing capability will enable dedicated virtual networks especially useful for mission-critical communications by infrastructure providers such as energy utilities. These mission-critical vertical use cases will pose more varied and onerous security requirements on the 5G network. For instance, it is likely that different network slices provided by the same service provider will have different security requirements.

5G builds and improves upon prior security measures and is fundamentally more secure than previous generations of mobile technology, offering specific security features to address issues that were present in 4G. Nevertheless, no system is totally secure and residual risks remain. For instance, 5G is more complex than previous generations, making more extensive use of the telco-cloud (including edge clouds), and involving more complex software (often cloud-native and container-based). The software supply chain is also more complex involving third parties and open-source software. All this makes for a more extensive attack surface for 5G than previous generations.

5G is flexible in terms of how security is implemented in deployment, which means that different networks may achieve different levels of security. Many 5G security features, as defined by 3GGP, are optional to use. Operators must make choices as to which of the range of standards-defined optional security features to enable in their deployed network. Examples include key strengths used for cryptography, and whether to employ optional user-plane integrity protection.

The operator must deploy the network in accordance with their own security architecture, addressing crucial aspects (outside the scope of standards or vendor offerings) such as how to partition the network (zoning, segmentation, security boundaries, etc.) and which systems to deploy in support of security operations (examples include security information and event management or SIEM, analytics, and vulnerability scanning). Employing zero-trust is one specific aspect of the security posture that an operator may choose to adopt.

Zero-trust

The principle behind zero-trust is that no access should be granted implicitly or by default. All access should be explicitly authenticated, authorized and monitored. Access privileges should be continually reviewed. A typical approach in the past was to authenticate user access to the local enterprise network, implicitly granting various levels of trust to users once inside. This over-reliance on perimeter security, together with coarse-grained management of trust, exposed enterprises to risks associated with advanced persistent threat agents (which can all-too-often breach perimeter security measures) and insider threat agents (which can potentially exploit their access privileges maliciously).

In addition to controlling initial access, zero-trust will also frustrate attempts by attackers to elevate privilege levels and to move laterally even if initial access is achieved. The monitoring aspect of zero-trust enhances the ability to detect malicious activity so the organization can react in real-time. Monitoring provides enhanced visibility and continuous oversight of access privileges and allows for more rapid correction of errors, thus reducing the organization's vulnerability to attack.

In addition to the original goal of bolstering user access security, the zero-trust principle can be applied to machine-to-machine interfaces as well. Ideally, all critical interface access should be subject to both authentication and fine-grained authorization, and all access should be monitored.

Firewalling and filtering are other aspects of access control in the domain of communications security. Application of zero-trust to communications security requires that all access is controlled at the finest possible level of granularity. Micro-segmentation of networks is an example of application of zero-trust in this context. With micro-segmentation, ideally all communication is explicitly filtered with no communication possible by default. In adherence to the principle of least-privilege, only authorized communications should be possible. Furthermore, monitoring of communications can provide oversight and afford opportunities for incident detection using anomaly detection techniques such as machine learning.

Applying zero-trust to 5G

Given the power of administrative functions in 5G, the potential consequences of unauthorized access to admin features are severe. Thus, zero-trust should be comprehensively applied to administrative user access including strong authentication, fine-grained authorization and ubiquitous monitoring. Ideally this will be augmented with user behavior analytics, potentially using AI/ML techniques. In particular, zero-trust should be employed for 5G management and orchestration (MANO) systems. A mature identity and access management (IAM) system, ideally with privileged access management (PAM) features, is a key enabler for this use of zero-trust.

Zero-trust principles should also be applied to interface and communications security in 5G. These include micro-segmentation of the cloud-native 5G network functions, possibly using software-defined networking (SDN) technology. All critical interfaces, including MANO and control messaging interfaces, should be secured using mutual authentication and fine-grained authorization. As defined by 3GPP, the 5G network standards allow for use of mTLS and OAuth to secure these interfaces. While the use of these is optional in deployment, it is strongly recommended that operators enable and use them to secure management interfaces and the 5G control plane. Since 5G will typically be deployed on the telco cloud, zero-trust should be applied in the hosting cloud infrastructure including for hosting operating systems, virtualization (whether hypervisor or container-based) and cloud management systems.

The Bell Labs Consulting approach

Bell Labs Consulting has supported communications service providers and regulators around the globe with risk assessments, security requirements and cybersecurity framework definition, including the application of the zero-trust security principle to 5G. Our risk-based approach, structured threat analysis methodology and cybersecurity knowledge base ensure that our clients have a robust foundation for planning the steps needed for elevating their security maturity over time.

Conclusion

Robust implementation of the zero-trust principle at all layers can significantly bolster the security posture of the 5G communications service provider. This is especially important for hosting new and evolving use cases such as the use of 5G network slices for mission-critical communications for infrastructure operators. Key technical enablers include IAM/PAM, advanced security analytics using AI/ML, micro-segmentation and network security mechanisms such as mTLS and OAuth. 5G communication service providers should roadmap their zero-trust journey based on a formal risk assessment to guide judicious choices of where and when to focus their security investments.

For further information please contact us: info.query@bell-labs-consulting.com

Learn more about Bell Labs Consulting at https://www.bell-labs.com/consulting/

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: 701051 (September) CID213560