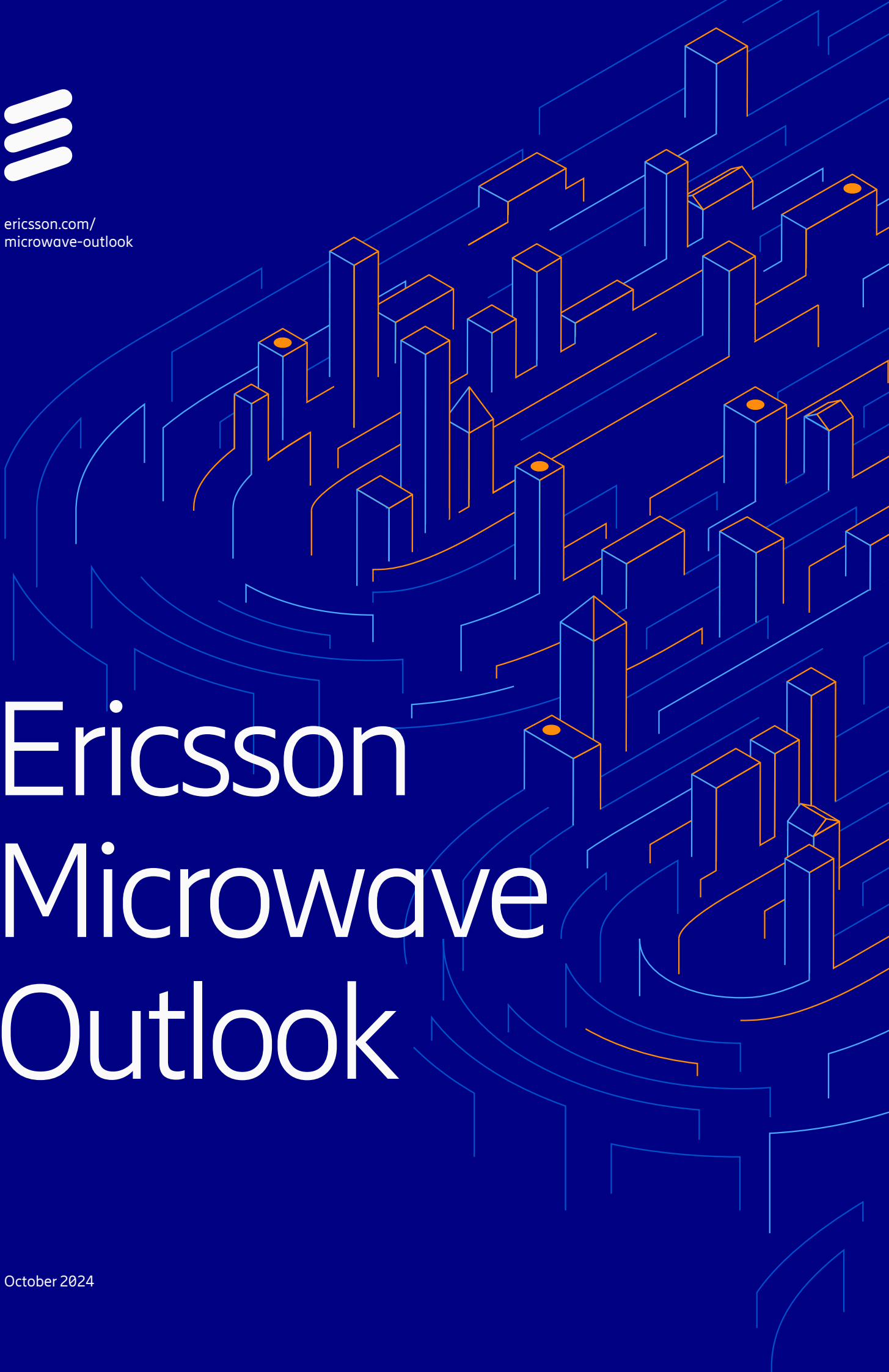


ericsson.com/
microwave-outlook

Ericsson Microwave Outlook

October 2024

Trusted microwave networks

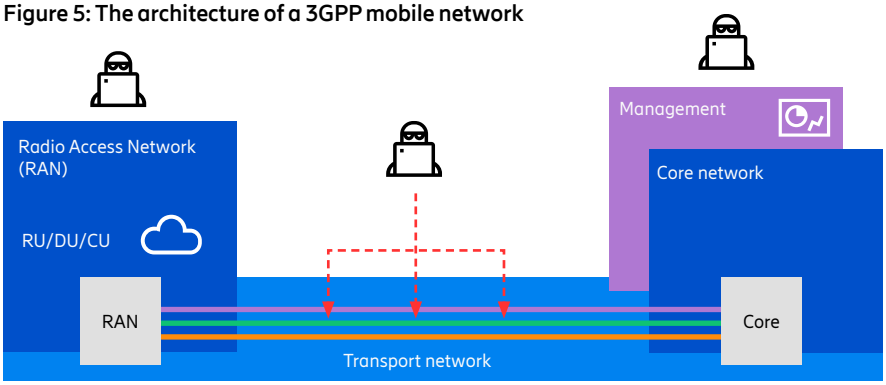
Today, mobile networks are one of the most vital parts of a nation's infrastructure and demands for trust, security and resilience are steadily increasing.

The security of a microwave transport network can be compromised in a multitude of ways. For example, full network access could be mistakenly given to contract workers hired to do a limited site upgrade. Perhaps a disgruntled former employee has access to team login credentials. A curious hacker could be exploring known Linux/open source vulnerabilities. Or, accidental access could be obtained by a used equipment trader who logs in to scrapped equipment that contains network information by testing default login credentials.

In recent years, the industry has responded to these potential risks by initiating and increasing focus on implementing vulnerability management processes and developing secure software and hardware architectures.

The active involvement of standardization bodies, such as the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA) in the US, and the National Cyber Security Centre (NCSC) in the UK, has also resulted in recent releases of various requirements and documents for network security.

Figure 5: The architecture of a 3GPP mobile network



Source: Ericsson (2024).

Threats and their mitigation in microwave networks

In Figure 5, the architecture of a 3GPP mobile network is shown, consisting of a Radio Access Network (RAN) with radio units (RU), distributed units (DU) and central units (CU) deployed in local sites, and the Core network deployed in a handful of national locations. The RU, DU, and CU are often located in unsupervised sites that may be exposed to unauthorized access, while the Core network is placed in high-security, data center-like locations. The transport network connects the RAN with the Core network and often consists of a mix of physical technologies, such as optical and microwave links that are able to cover long distances with many nodes. The nodes are frequently located in remote, unsupervised locations which can be susceptible to unauthorized access, thereby providing possibilities for eavesdropping, ingestion of manipulated software, attacks via vulnerable third-party providers (3PPs), hidden activities and denial of service attacks (Figure 6).

Unauthorized access

In this article, an unauthorized access event is defined as one where a user without access rights gains admission to information or configuration rights in a node or a network by having access to physical hardware or login credentials. To mitigate this, it is essential to implement strong access control policies with a centralized authentication process requiring individual, strong passwords that are frequently updated, and for this to be combined with multi-factor authentication.

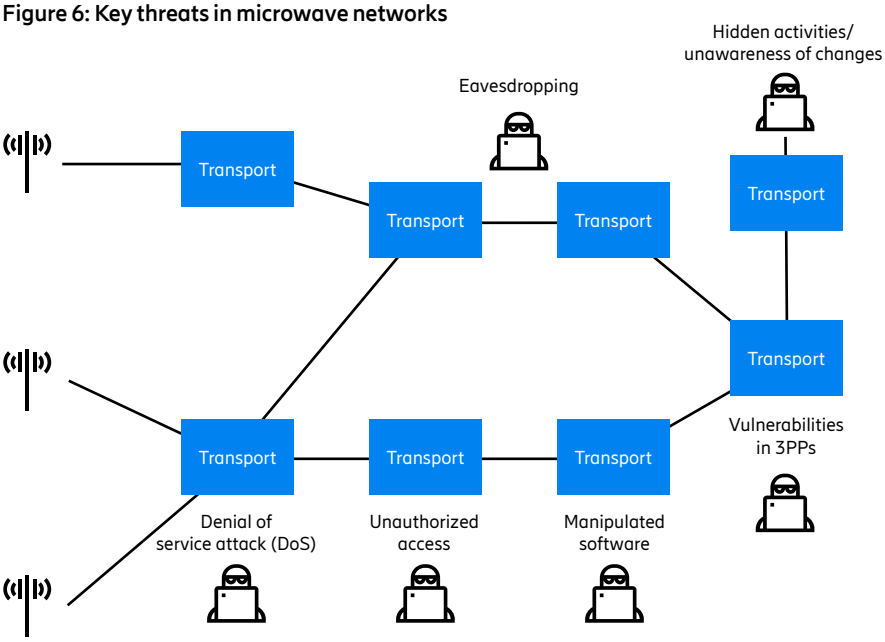
Future enhancements are being discussed across the industry to make it more difficult for external sources to access unauthorized information directly through physical hardware. For instance, to prevent intrusion by probing memory chips or the communication lines between different chips on a printed circuit board, the hardware should be built on a trusted hardware architecture. The intent is that components in the system should have a wall of protection against other components in the system, which prevents unauthorized access to the complete system if one component becomes implicated. This could, for example, mean that communication between hardware components is encrypted and that data is authenticated. An intuitive way to understand the difference between a common hardware architecture and a trusted hardware architecture is a comparison between a coconut and a pomegranate. The coconut has a hard shell protecting the content inside but once the shell is penetrated, it is possible to access its content. The pomegranate, on the other hand, has protective shells around all components within its outer shell.

Eavesdropping

The signal in a microwave network is similar to the signal from the RAN, propagating through an unprotected medium, namely the air, but it is still a rather complex task to intercept the traffic in mid-air. It requires detailed knowledge about the transmitted signal such as the frequency, modulation, data rates and coding of the transmitted data, which is proprietary to each vendor. Still, data encryption is recommended to protect the network from eavesdropping. End-to-end encryption, specifically encryption and decryption in the

Core network and the RAN nodes, is the recommended solution. It is also transparent to individual proprietary link technologies, ensuring the information remains encrypted throughout the full transport network. Another option for microwave is radio link encryption, which encrypts the signal and provides the benefit of being impossible to detect if or when the radio link is being used. However, if only radio link encryption is used, there is still a vulnerability at each node where decrypted information may be monitored if an unauthorized user is getting access to the node. Hence, the recommendation is to have end-to-end encryption with the option to add radio link encryption to protect the network even further.

Figure 6: Key threats in microwave networks



Source: Ericsson (2024).

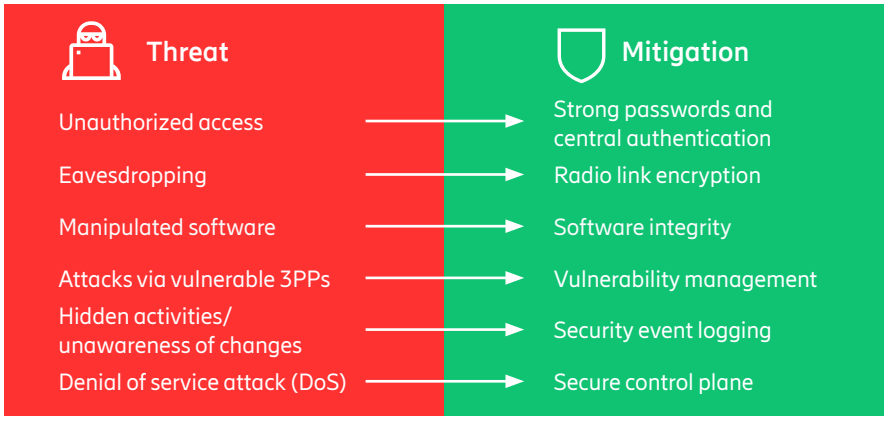
Manipulated software
A complex threat involves the intentional manipulation of firmware running on microwave nodes. To address this, the microwave vendor must secure software integrity through automatic or manual updates of software from trusted sources, using secure protocols. Furthermore, it is important to implement solutions that can secure the trust of the updated software, such as ensuring users of systems can be certain that downloaded and booted software is not altered in any way, and that it is digitally signed by the microwave vendor.

Attacks via vulnerable 3PPs
Nowadays, 3PP software components, such as Linux distributions and 3PP network stacks, are an integral part of modern software development. Vulnerability management – including control, tracking, assessment of impact and mitigation of known and recently detected vulnerabilities in the 3PP software components – is, therefore, crucial, as information about these vulnerabilities can quickly spread and provide simple and straightforward opportunities for attackers to target and explore.

Microwave vendors should have a clear strategy for discovering, tracking and addressing vulnerabilities in their equipment as part of their product development life cycle and a well-defined process for sharing known vulnerabilities with service providers. This strategy must comply with standards such as the 3GPP Network Equipment Security Assurance Scheme, monitored by organizations like GSMA.[1]

Hidden activities/unawareness of changes
To limit the impact of an intrusion, it is of the utmost importance to detect attacks and security vulnerabilities as soon as possible. One example is the detection of intentional or unintentional changes in security settings that may lead to malicious activity, such as hidden configuration changes of the node. To mitigate this, it is necessary to support security event logging on the microwave nodes, which enables visibility of security events and activities.

Figure 7: Summary of security threats and mitigation actions



Denial of service (DoS) attack
In a DoS attack, a node is flooded with requests, the aim being to make the node inaccessible and thereby impact network performance. To mitigate this, microwave nodes should have the ability to enable policies in the control plane to prevent the build-up of request queues, which ensures that the network node continues to operate. One option for achieving this could be a policy allowing the service provider to configure a quality-of-service filter that manages the traffic flow of control plane packets to protect the microwave node. Securely configured microwave nodes are essential for the proper operation of microwave networks, and both vendors and service providers play vital roles in ensuring that the necessary security functions and hardening measures are in place.

Conclusion
This article provides insights into the rapidly evolving security landscape and highlights some common security threats and their mitigations, which are summarized in Figure 7. Service providers can mitigate these threats through diligent security configurations, and should also consider security features when selecting hardware. Future security improvements may involve changes in trust boundaries, requiring comprehensive security design and secure communication between internal platform components.

Overall, building reliable microwave networks requires both collaboration and standardization to address security challenges and enable swift adaptation to evolving security requirements.

[1] Network Equipment Security Assurance Scheme (NESAS) – Industry Services (gsma.com).

About Ericsson

Ericsson's high-performing, programmable networks provide connectivity for billions of people every day. For nearly 150 years, we've been pioneers in creating technology for communication. We offer mobile communication and connectivity solutions for service providers and enterprises. Together with our customers and partners, we make the digital world of tomorrow a reality.

www.ericsson.com

Ericsson
SE-164 80 Stockholm, Sweden
Telephone +46 10 719 0000
www.ericsson.com

EAB-24:006645 Uen