AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

SECURING THE FUTURE

Ensuring 5G Network Security

Martin Stierle

AUSTRIAN INSTITUTE OF TECHNOLOGY

BMK

1.465 employees

7 Centers

Austria‘s largest RTO

Applied Research

Infrastructure Systems

System Competence

Federation of Austrian Industries (through VFFI)

Next Generation Solutions

4 Subsidiary Enterprises

LKR, NES, SL, Profactor 51%

182,9 m EUR total revenue

Tomorrow Today

as of YE 2022

INTRODUCTION

- The era of 5G, is promising ultra-fast speeds, low latency, and massive connectivity, and the potential for transformative applications across industries.

- Kubernetes has emerged as a cornerstone for deploying and managing the complex network functions required to support 5G services.

- 5G security is improved over its predecessors 3G and 4G but new attack vectors are emerging.

- Virtualization and cloud security pose a new challenge in modern 5G networks.

SECURING THE FOUNDATION: IMPORTANCE OF SECURITY IN 5G NETWORKS

Expanded Attack Surface

- Increased connectivity, diverse devices including IoT

Critical Infrastructure

- Supports critical infrastructure and essential services, including healthcare, transport, energy, finance,…

Data Privacy Concerns

- Handles vast amounts of sensitive data, including personal, financial, and proprietary information

Regulatory Compliance

- Compliance with regulatory requirements and industry standards, such as GDPR, NIS, and PCI DSS

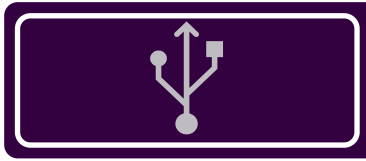
SECURITY CHALLENGES IN 5G NETWORKS

Evolving Threat Landscape

- Dynamic nature of cyber threats, including malware, ransomware, phishing attacks, and zero-day exploits

Vulnerabilities in Network Elements

- Complex ecosystem, including base stations, core networks, edge computing nodes, and IoT devices



Insider Threats and Misconfigurations

- Insider threats, human errors, and misconfigurations

Virtualized 5G networks

- Multi-Tenancy Security, Virtual Network Function (VNF) Security, Network Slicing Security, Hypervisor Security

OVERVIEW OF SECURITY THREATS

Cyberattacks	Emerging Threats	IoT Vulnerabilities	Supply Chain Risks	Computing Platform Risks
• Distributed denial-of-service (DDoS) attacks • Ransomware • Malware • Man-in-the-middle attacks	• AI-Powered Attacks • 5G-specific Vulnerabilities	• Device hijacking • Botnet infections • Insecure communication protocols	• Compromised hardware, software, or firmware	• Pod and container breakout • Privilege escalation • Denial-of-service

Cyberattacks on 5G networks can disrupt essential services and can result in data breaches, identity theft, and privacy violations. This emphasizes the need for robust security measures and resilience.

SECURITY MEASURES IN 5G NETWORKS

Encryption

- Strong encryption algorithms to protect data transmission and communication channels in 5G networks

Authentication

- Strong authentication mechanisms, including mutual authentication and certificate-based authentication, to verify the identity of network entities, users, and devices

Access Control

- Granular access control policies, role-based access control (RBAC), and least privilege principles
- Network segmentation techniques to isolate and protect sensitive assets.

Network Slicing

- Leverage network slicing capabilities in 5G networks to create isolated virtual networks with dedicated resources, security policies, and performance characteristics for specific applications.

CONCLUSIONS

- Security in 5G networks is essential for safeguarding against emerging threats and ensuring the integrity, confidentiality, and availability of networks and services
- Overall 5G specifications define a system with a high level of security
- Attacking 5G protocols requires powerful attackers with great expertise
- Easier to attack
  - Underlying infrastructure like Kubernetes
  - Lateral movement from IT in enterprise network to 5G core using e.g.stolen credentials

- The complexity of Kubernetes environments and common security risks, such as vulnerabilities in container images and misconfiguration, are key challenges in securing 5G networks.

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THANK YOU!

Martin Stierle, 2024-4-18