数智创新
变革未来

5G网络虚拟化安全风险

目录页

Contents Page

软件定义网络（SDN）架构的安全隐患

软件定义网络（SDN）架构的安全隐患

控制器中心化风险

- SDN控制器集中控制网络流量，成为单点故障点，一旦被攻破，整个网络面临瘫痪风险。
- 控制器本身可能成为攻击目标，如DDoS攻击、恶意软件感染等，影响网络可靠性。

数据平面可编程性

- SDN允许应用程序对数据平面进行编程，扩大攻击面，攻击者可利用安全漏洞发起拒绝服务攻击或数据窃取。
- 复杂的网络配置和自动化工具可能引入新的安全隐患，增加误配置的风险。

软件定义网络（SDN）架构的安全隐患

虚拟化技术风险

- SDN中虚拟化技术（如虚拟交换机）增加了攻击面，攻击者可通过虚拟化技术实现网络中断或数据窃取。
- 虚拟化管理程序的漏洞可能被利用，影响整个网络的安全。

缺乏传统安全机制

- SDN架构缺乏传统安全机制，如防火墙、入侵检测系统，增加了网络遭受攻击的可能性。
- SDN控制器缺少访问控制机制，无法有效监测和控制网络流量。

软件定义网络（SDN）架构的安全隐患

供应链风险

- SDN基础设施的供应商可能会引入安全隐患，例如恶意代码、后门程序。
- 供应商的漏洞可能会被利用，影响使用 SDN 架构的网络安全。

管理和监控挑战

- SDN架构的复杂性增加了管理和监控的难度，安全专家难以及时发现和应对安全威胁。
- SDN控制器缺乏可视性和审计功能，难以跟踪网络活动和检测异常行为。

容器技术的安全风险评估

容器技术的安全风险评估

主题一：容器逃逸和特权提升

1. 容器逃逸指恶意代码突破容器的隔离机制，执行容器外系统命令或访问敏感资源。
2. 特权提升是指恶意代码在容器内获得更高权限，从而控制主机或其他容器。

主题二：容器镜像安全

1. 容器镜像包含应用程序代码和依赖项，可能存在恶意软件、后门或安全漏洞。
2. 应定期扫描和验证镜像，以确保安全性和完整性。

容器技术的安全风险评估

主题三：容器编排和管理平台安全

1. 容器编排和管理平台负责调度和管理容器，存在配置错误、身份验证和授权漏洞的风险。
2. 应强化安全设置，实施访问控制和审计机制。

主题四：容器内的隔离

1. 容器隔离机制旨在将容器与其他容器和主机隔离，防止恶意代码传播。
2. 应采用强有力的隔离技术，例如特权分离、名前空间和资源限制。

容器技术的安全风险评估

主题五：供应商锁定

1. 不同容器供应商的实现可能存在差异，导致安全风险和管理挑战。
2. 应评估供应商的安全性、支持和互操作性，并考虑使用开放源代码或标准化解决方案。

主题六：供应链攻击

1. 容器供应链包括组件供应商（例如镜像库）、构建工具和管理平台。

5G虚拟化网络中DDoS攻击的防控策略