Rialtas na hÉireann
Government of Ireland

Electronic Communications Security Measures

007 – Virtualisation Security v1.0

2021

Prepared by Department of the
Environment, Climate & Communications
gov.ie/decc

Table of Contents

Table of Contents i

1 Foreword 3

2 Introduction 4

3 Scope 4

4 References 4

5 Definitions, Symbols and Abbreviations 5

5.1 Definitions 5

5.2 Symbols 7

5.3 Abbreviations 7

6 Overview of Risk 9

6.1 Introduction 9

6.2 Types of Virtualisation 10

6.3 Virtualisation Deployment Scenarios 11

6.4 Administration of the Virtualisation Layer 12

6.5 Virtualisation Layer Compromise 12

6.6 Geographic Issues 13

6.7 Management and Orchestration (MANO) 13

6.8 Container Security 14

7 Security Measures 15

8 Implementation Guidance 18

9 Relevant References 19

9.1 ENISA: The security aspects of virtualisation 19

9.2 ENISA: Threat Landscape and Good Practice Guide for Software Defined Networks/5G 19

9.3 GSMA: FS.33 Network Function Virtualisation Threats Analysis 19

9.4 GSMA: Considerations, Best Practices and Requirements for a Virtualised Mobile Network 20

9.5 3GPP: TR 33.4848 v0.6.0 (2019-11) Study on Security Impacts of Virtualisation (DRAFT) 20

9.6 NIST: SP 800-125 Guide to Security for Full Virtualisation Technologies 21

9.7 NIST: SP 800-125B Secure Virtual Network Configuration for VM Protection 21

9.8 NIST Special Publication 800-190 Application Container Security Guide 21

9.9 ETSI: Industry Specification Group (ISG) Network Functions Virtualisation (NFV) 21

1 Foreword

The Electronic Communications Security Measures (ECSMs) have been produced by the Electronic Communications Security Measures working group convened by the Irish National Cyber Security Centre (NCSC), which forms part of the Department of the Environment, Climate and Communications (DECC); and with the support of the Commission for Communications Regulation (ComReg). Industry participation in the WG has involved network operators, including the Mobile Network Operators (MNO) which have been awarded 5G licences, and selected fixed line operators.

This ECSM is part of a series of documents listed below:

Title	Subject
ECSM 001	General
ECSM 002	Risk Management
ECSM 003	Physical and Environmental Security
ECSM 004	Training, Awareness and Personnel Security
ECSM 005	Network Management & Access Control
ECSM 006	Signalling Plane Security
ECSM 007	Virtualisation Security
ECSM 008	Network, Monitoring and Incident Response
ECSM 009	Supply Chain Security
ECSM 010	Diversity, Resilience & Continuity
…	…

2 Introduction

Ireland's modern digitally connected society and economy is highly dependent on reliable and secure electronic communications networks and services (ECN and ECS respectively). They form the backbone of much of Ireland's critical national infrastructure providing connectivity to the essential services upon which citizens rely, such as healthcare providers, energy providers, financial institutions, emergency services and public administration. It is of paramount importance that these vital networks and services are protected from the full range of threats with an appropriate level of technical and organisation security measures.

The ECSM Working Group Convened on the 06th 07th and 08th of October 2020 to discuss matters concerning virtualisation security. The group heard from experts in the field of virtualisation security and held focussed discussions on the risks, challenges and best practices associated with virtualisation security as it pertains to telecommunications networks. ECSM 007 –Virtualisation Security has been developed by the NCSC informed by those meetings.

3 Scope

The security measures set out in this ECSM are applicable to all providers of public electronic communications networks and electronic communications service which have implemented virtualisation as part of their operational network deployments.

The legislative basis for the ECSMs is set out in ECSM 001- General

4 References

Document	Title
3GPP TR 33.848	Study on Security Impacts of Virtualisation (DRAFT v0.6.0)
ENISA	Technical Guideline on Security Measures under the EECC
ENISA	Supplement to the technical guideline on Security Measures under the EECC
ENISA	The Security Aspects of Virtualisation

ENISA	Threat Landscape and Good Practice Guide for Software Defined Networks/5G
GSMA FS.33	Network Function Virtualisation Threats Analysis
ISO/IEC 27001:2013	Information technology — Security techniques — Information security management systems — Requirements
ISO/IEC 27002:2013	Information technology — Security techniques — Code of practice for information security controls
NIST	Framework for Improving Critical Infrastructure Cybersecurity v1.1
NIST SP 800-100	Information Security Handbook: A Guide for Managers
NIST SP 800-125	Guide to Security for Full Virtualisation Technologies
NIST SP 800-125B	Secure Virtual Network Configuration for VM Protection
NIST SP 800-190	Application Container Security Guide
NIST SP 800-53 R4	Security and Privacy Controls for Federal Information Systems and Organizations

31

32 5 Definitions, Symbols and Abbreviations

33 5.1 Definitions

Term	Meaning
EU 5G Security Toolbox	Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures' document published jointly by member states on 31st of January 2020
EU Risk Assessment	EU coordinated risk assessment of the cybersecurity of 5G networks report published jointly by the EU

	Member States on 09th October 2019
Host	A computer or other device that communicates with other hosts on a network. Hosts on a network include clients and servers that send or receive data, services, or applications.
Hardening	The process of securing a system by reducing its surface of vulnerability, reducing available means of attack. This typically includes changing default passwords, the removal of unnecessary software, unnecessary usernames or logins, and the disabling or removal of unnecessary service.
Hyperjacking	An attack in which a hacker takes malicious control over the hypervisor that creates the virtual environment within a virtual machine host
Kernel	A computer program at the core of a computer's operating system that has complete control over everything in the system.
National Risk Assessment	Risk assessment carried out by the National Cyber Security Centre and forwarded to the European Commission on 15 July 2019.
Noisy neighbour problem	When a VM accessing shared resources uses more than it should. This causes other VMs accessing those resources to suffer from reduced or erratic performance
Orchestration	A set of processes that collectively automate the management and control of digital information systems.
Scaling	The ability to dynamically extend/reduce resources granted to virtual elements as needed

Scaling out/in	The ability to scale by add/remove resource instances
Scaling up/down	The ability to scale by changing allocated resource, e.g., increase/decrease memory, CPU capacity or storage size
Trust Domain	A collection of entities that share a set of security policies
Trusted Platform Module	Trusted Platform Module (TPM, also known as ISO/IEC 11889) is an international standard for a secure crypto processor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys.
Virtualisation	The process of abstracting a resource beyond its physical form. Many types of technologies can be virtualised, including servers, storage devices, networks, network functions and applications.
Virtualisation Infrastructure	The totality of all hardware and software components that build up the environment in which virtualised elements are deployed
Virtual Machine	Virtualised computation environment that behaves very much like a physical computer/server

5.2 Symbols

Nil

5.3 Abbreviations

Term	Meaning
BMC	Baseboard Manager Controller
ComReg	The Commission for Communications Regulation
COTS	Commercial off the shelf

DECC	The Department of Environment, Climate and Communications
ILO	Integrated Lights Out
ECSM	Electronic Communications Security Measures
MANO	Management and Orchestration
MNO	Mobile Network Operator
NCSC	National Cyber Security Centre
NF	Network Function
NFV	Network Function Virtualisation
OS	Operating System
RAS	Reliability, Availability, Serviceability
TPM	Trust Platform Module
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNF	Virtual Network Function

37

38

6 Overview of Risk

6.1 Introduction

In computing, virtualisation encompasses a number of different techniques to create a virtual, or software version of a computing device. Examples of devices and systems which may be virtualised include hardware platforms, memory, storage, or an entire network. Network Function Virtualisation (NFV) refers to the deployment of Network Functions (NFs) as software modules which run on commercial off the shelf (COTS) hardware. This contrasts with the traditional deployment of network components as specialised hardware devices.

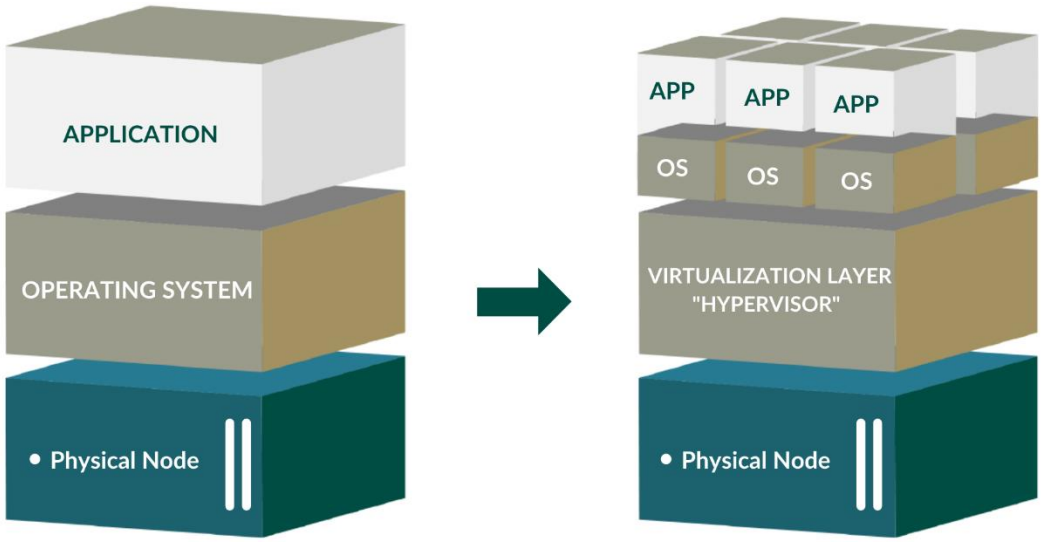

Figure 1 - Virtualisation[1]

Virtualisation is a fundamental building block of next generation networks and while not the only way of implementing a 5G network, it is nevertheless the primary implementation method being pursued to some degree by operators and manufacturers. Additionally, virtualisation is being applied to earlier generations of networks, such as 4G, and part virtualised networks containing a mixture of physical, containerised, and virtualised network functions will be commonplace for most operators for the foreseeable future.

Virtualisation techniques, while providing clear advantages to security, also come with increased security risks that must be taken into account when deploying a strong and secure virtualised infrastructure.

[1] https://www.researchgate.net/figure/Virtual-vs-Traditional-Architecture-There-are-different-types-of-hypervisor-which-provide_fig1_323918941

6.2 Types of Virtualisation

One of the attractions of virtualisation is that it allows resources to be used flexibly. Sharing hardware resources between VNFs allows networks to scale services up and down as required and to centralise the management and orchestration.

However, the adoption of shared resources raises security questions which do not apply when using discrete physical infrastructure. In particular, virtualisation technology needs to ensure that VNFs can be isolated from one another, particularly in the case where they have specific security requirements. There are various approaches to isolating VNFs, ranging from using physically separate hardware to using separate containers. From a security perspective, there are four main types of virtualisation, with increasing levels of security

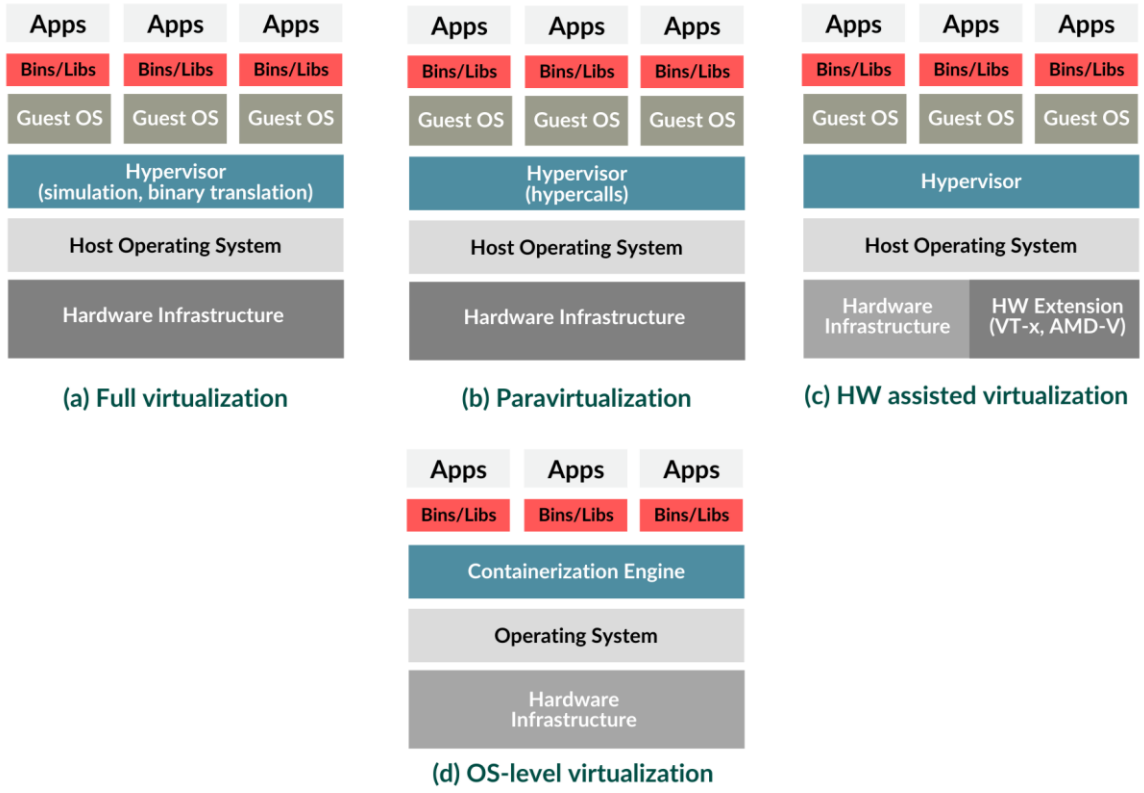

Figure 2 – Types of Virtualisation[2]

- **OS-Level virtualisation**: Also known as 'containerisation' where the separation between workloads is performed by the kernel on the host through a containerisation engine. In this case, compromise of the host's kernel is enough to compromise the host and co-hosted workloads.

[2] ENISA: Security aspects of virtualization https://www.enisa.europa.eu/publications/security-aspects-of-virtualization

- **Para-virtualisation**: The hypervisor can be bypassed with ‘hypercalls’ for efficiency reasons which allow the guest OS to directly address the hardware. In this case, compromise of a ‘hypercall’ may be enough to compromise the host and co-hosted workstreams.
- **Full virtualisation**: In full virtualisation, the hypervisor performs the security separation. In this case, a hypervisor breakout is required to compromise the host and co-hosted workstreams.
- **Hardware-backed virtualisation:** Security can be increased through the use of hardware backed enforcement of separation mechanisms. (e.g., Input Output Memory Management Unit filtering (IOMMU) protections such as Intel’s VT-d // VT-x and AMD’s AMD-V // AMD-Vi).

It is expected that vulnerabilities in the kernel or within a para-virtualisation environment will occur relatively frequently, and hence the first two types are not appropriate for use as a security barrier. Where this type of virtualisation is used, virtual workloads from different trust domains should not run on the same host.

On the other hand, full virtualisation does allow a level of security separation between virtual machines. From a security perspective, full virtualisation provides the greatest flexibility in terms of host deployment. However, it should be noted that a host compromise will compromise all workloads running on that host as such the admin of the underlying hardware (the RAS/BMC/ILO type functionality) is as critical as the admin of the virtualisation layer.

6.3 Virtualisation Deployment Scenarios

There are various deployment scenarios for virtualised infrastructure, with varying levels of risk. It ranges from a situation where an operator controls and owns their own virtualised infrastructure, shares the infrastructure with their parent group, or hosts their infrastructure in a third-party cloud provider. In a third-party environment, an operator could share their environment with competing operators, or non-telecommunication related services. In such a situation the network could be exposed to network traffic from entities with a lower overall level of security.

Multi-tenant virtualisation infrastructures present a risk that without adequate separation controls, the security or performance of their VNFs, could be compromised by other tenants of the environment, either maliciously or through the "noisy neighbour problem"[3]

Obviously, the use of any third-party hosting for VNFs would need to be carefully managed as outlined in ECSM 009 – Supply Chain Risk Management, ensuring that the outsourcing of hosting does not result in a lowering of the overall security and the provider meets the requirements set out in the ECSM series.

6.4 Administration of the Virtualisation Layer

A key aim of virtualisation is implementation of the network using flexible resources which can be scaled and sized in near real-time to fit customer demand. To achieve this effectively, NFV deployments rely on a single administration domain, where an administrator with root access is able to manage the hosts and NFV environment. Without extra security controls, an attacker who gains access to one of these accounts would be able to exploit, control and manage the entire NFV environment.

Most virtualisation platforms make it possible for a user with root access to the virtualisation layer to view and edit the memory of hosted VMs. This administrator may be able to change or stop processes running in the VM, give other applications access to the VM or steal security critical data.

An attacker may have access to the virtualisation layer via a variety of means. The access could be from a rogue employee at the hosting company or could be more illegitimate (see below). From the point of view of the VNF these attack vectors are the same, as both results in a rogue actor gaining access. In general, such access would be invisible to the VNF.

6.5 Virtualisation Layer Compromise

As a single point of failure, the hypervisor presents a uniquely high risk to network security in the event that they contain vulnerabilities. While hypervisor vulnerabilities are not common, the impact of one occurring can be devastating to network security. Gaining access to the hypervisor would be catastrophic and give an attacker access to all workloads running above the hypervisor. Such an attack is called 'VM Breakout' or 'Hyperjacking' and has been

[3] When a VM accessing shared resources uses more than it should. This causes other VMs accessing those resources to suffer from reduced or erratic performance

demonstrated to be possible.[4]

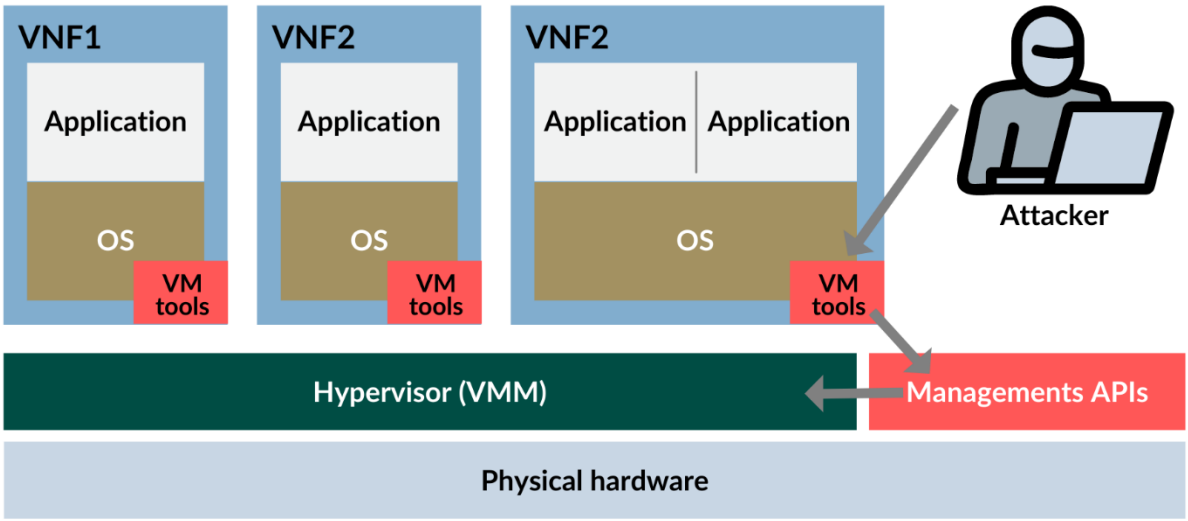

Figure 3 – VM Breakout Attack[5]

To prevent a VM from impacting other VMs or hosts, it is a good practice to separate VM traffic and management traffic. This will prevent attacks by VMs tearing into the management infrastructure. It is also a good idea to separate the VLAN traffic into groups and disable all other VLANs that are not in use. Likewise, VMs of similar functionalities can be grouped into specific zones and their traffic should be isolated. Each zone can be protected using access control policies and a dedicated firewall based on the necessary security level.

6.6 Geographic Issues

In traditional physical based networks, operators know where subscriber or other sensitive data is located. However, virtual networks are designed in a way whereby such data can be anywhere in the hosted environment, potentially spanning multiple data centres or legal jurisdictions. In such a setup operators may encounter challenges in meeting legal obligations to data protection and lawful interception legislation. It is important that even in virtualised infrastructures, the operator has a clear picture of where sensitive data actually physically resides and that it is appropriately protected.

6.7 Management and Orchestration (MANO)

One of the major advantages of virtualised networks is the ability to dynamically scale network capacity out/in and up/down and to continuously adapt to network demands. A

[4]‘ Cloudburst: Hacking 3D (and Breaking Out of VMware) https://www.blackhat.com/html/bh-usa-09/bh-usa-09-speakers.html

[5] http://www.anastacia-h2020.eu/publications/NFV_Security_Threats_and_Best_Practices.pdf

dynamically scaled network can present challenges due to the complexity of the system with a risk of configuration errors having significant impacts on the security of the network. The orchestration tools currently available provide the ability to deploy infrastructure and services from code. This approach provides a fully reproducible and automatable method of building and scaling a network in a secure and understood way, while limiting errors caused by human interaction.

Using modern development tools and techniques such as code versioning, continual integration, and delivery pipelines allows for rapid prototyping and testing of new features, security patches, and changes, without impacting the network availability in a wider manner as any changes can be tested at a small scale and quickly rolled back if there are any negative consequences. Deploying services and infrastructure as code is the recommended way of building out networks and services.

With the move to rapid prototyping and configuration as code, operators should implement similar levels of control to these code repositories as they do to the configuration of hardware and other security critical functions.

As the MANO is responsible for on-boarding, instantiation, and lifecycle management of all VNFs within a virtualised network, it represents a single point of failure and an attractive target for attackers. The system should be deployed in such a way as to provide isolation and redundancy to increase the defence against a single point of failure. The MANO should not reside on the same infrastructure as it controls. MANO functions should include internal health checks to detect potential intrusion and take protective actions.

6.8 Container Security

Recently, application virtualisation has become increasingly popular due to advances in its ease of use and a greater focus on developer agility as a key benefit. In application virtualization, the same shared OS kernel is exposed virtually to multiple discrete apps. OS components keep each app instance isolated from all others on the server. In this case, each app sees only the OS and itself, and is isolated from other apps that may be running on this same OS kernel.

The key difference between OS virtualization and application virtualisation is that with application virtualisation, each virtual instance typically runs only a single app. Today's application virtualization technology is primarily focused on providing a portable, reusable, and automatable way to package and run apps. The terms application container or simply container are frequently used to refer to these technologies. The term is meant as an

analogy to shipping containers, which provide a standardized way of grouping disparate contents together while isolating them from each other.

Whilst containers offer increased agility and flexibility, the level of separation provided by the kernel is not equivalent to full virtualisation. Therefore, containers should not be used to separate sensitive workloads.

Covering the full range of security risks associated with containers, goes beyond the scope of this document, however standards such as NIST SP 800-190 provide guidance on this topic. The document highlights the risks associated with Image Risks, Registry Risks, Orchestrator Risks, Container Risks and Host OS Risks, including recommending a series of countermeasures that can be taken to mitigate the risks.

7 Security Measures

The operator should implement the Virtualisation Security Measures in a manner that is customised to be appropriate and proportionate to the organisation.

Measure	Description
Understanding the Virtual Environment	
VS.01	The operator shall retain sufficient expertise to manage the virtualised infrastructure.
VS.02	The operator shall understand the virtual network, including data flows, trust domains and the location and status of the physical hosts on which the virtual network resides.
Secure Infrastructure	
VS.03	The hardware & software involved in providing the virtualisation infrastructure shall be kept up to date with regular security patches to known vulnerabilities.
VS.04	The hardware providing the virtualisation infrastructure shall support silicon chip-based security functionality with a trusted platform module (TPM) that stores measurements of the entire virtualisation layer and boot process.
VS.05	The hardware providing the virtualisation infrastructure shall be hardened. Communication between physical hosts shall be restricted to the minimum necessary. Interfaces shall be restricted to trusted hosts and hard-coded

	configurations shall be reduced to the minimum necessary.
VS.06	Sensitive virtual workloads or those providing a security boundary should not directly address the physical hardware on which they run. Exceptions shall be documented, risk assessed and justified.
Secure Virtualisation Layer	
VS.07	The software providing the virtual infrastructure, such as the hypervisor and Host OS, shall be hardened and kept up to date with regular security patches to known vulnerabilities.
VS.08	The virtualisation layer shall be validated during boot up using a TPM.
VS.09	The virtualisation layer shall be hardened. Only the minimum services and processes necessary to operate VNFs shall be included, and other services shall be removed by default.
VS.10	The virtualisation layer shall be monitored to detect potential intrusion and take protective actions.
Trust Domains and Separation	
VS.11	Virtual workloads shall be allocated a trust domain based on their sensitivity. Trust domains shall be separated using full virtualisation - containers shall not be used to separate trust domains.
VS.12	Physical hosts shall be categorised into security pools based on risk[6]. The pools shall be tagged with the trust domains that they can execute, in order to ensure sensitive functions are not executed in physically exposed locations where the risks associated with compromise of a host is increased (such as the network edge or shared data centres).
VS.13	The MANO represents a critical part of an operator's virtual network deployment and shall be provided with enhanced level of security protection and monitoring.

[6] The risk may be based upon, inter alia, the host type, the security features of the host, and the location or environment within which that host resides.

Secure Administration	
VS.14	Administration of the virtualisation infrastructure or the MANO function represents the highest level of access. The security measures outlined in ECSM 005 – Network Management and Access Control around privileged access shall apply to the administration of the virtualisation infrastructure.
VS.15	Changes to the virtualisation infrastructure shall follow appropriate change management procedures including authorisation and documentation.
VS.16	Administration of the virtualisation infrastructure or MANO should be automated wherever possible, in order to reduce configuration errors and reduce opportunities for malicious actors.
VS.17	The code used for automated administration shall be stored securely and shall be monitored and audited. Changes to the code should require peer review and two person sign off.
VS.18	Administrators of the virtual infrastructure should not have access to the workloads within the virtualised environment. Exceptions shall be documented, risk assessed and justified.
VS.19	Administrators should only be provided with the privileges and access that is required for their role.

198

199

8 Implementation Guidance

Operators should take a policy-based approach to the security of their virtualised infrastructure ensuring that the security measures are implemented consistently at an organisational level.

The security measures outlined above provide the minimum baseline security standards expected in order to mitigate the main risks identified to virtualised networks. In order for operators to meet the Security Measures set out in this document, they should design and implement security policies based upon the recommendations set out in appropriate international standards or technical specifications. A non-exhaustive overview of some of the main standards and guidance documents is provided below.

As most of the electronic communications industry is at an early stage in the deployment of virtualisation it is intended that this ECSM will be reviewed and updated periodically in order to keep abreast of security best practices, as the technology develops and evolves..

9 Relevant References

The following standards, guidelines and reports offer further detail and will assist operators in designing policies, procedures and processes that meet the *Security Measures* outlined in Section 7 of this document.

9.1 ENISA: The security aspects of virtualisation

https://www.enisa.europa.eu/publications/security-aspects-of-virtualization

This research paper by ENISA provides an in-depth analysis into all of the security aspects of virtualisation. The paper gives a history and overview of virtualisation and current implementations. The paper highlights the main threats, vulnerabilities, risks, and impacts associated with virtual environments. Finally, the paper outlines a series of virtualisation good practices. In total the paper recommends 82 controls covering General-purpose good practices (Physical Layer, General, Configuration) and Component-specific good practices (Guest/Host OS, Containers, Hypervisor & VNM[7], Virtual network, Virtual Storage).

9.2 ENISA: Threat Landscape and Good Practice Guide for Software Defined Networks/5G

https://www.enisa.europa.eu/publications/sdn-threat-landscape

This study reviews threats and potential compromises related to the security of SDN/5G networks. More specifically, this report has identified related network assets and the security threats, challenges and risks arising for these assets. Driven by the identified threats and risks, existing security mechanism and good practices for SDN/5G/NFV has been identified. Finally based in the collated information technical, policy and organizational recommendations for proactively enhancing the security of SDN/5G is provided.

9.3 GSMA: FS.33 Network Function Virtualisation Threats Analysis

https://www.gsma.com/security/resources/fs-33-network-function-virtualisation-nfv-threats-analysis/

***Restricted to GSMA Members.**

This document provides a comprehensive overview of the threats related to NFV and the underlying infrastructure and platforms hosting the NFV.

[7] MANO

The virtualization of network functions can be realized in several different ways and to varying degrees. A Virtualised Network Function (VNF) can be a complex virtual appliance running a complete operating system populated with several applications. It may have multiple layers of interaction and functionality and, in some instances; it may even have specific hardware requirements.

A VNF can also be an isolated singular function running on a thin container-based kernel and have very limited interaction with its surrounding network entities. Containers, while being streamlined and generally smaller than more traditional virtual machines are exposed to the same NFV environment and suffer from the same vulnerabilities. In this document they are therefore treated as virtual machines and covered by the same risks and mitigation techniques if nothing else is stated in the risk or mitigation description itself.

9.4 GSMA: Considerations, Best Practices and Requirements for a Virtualised Mobile Network

Virtualisation.pdf (gsma.com)

This document outlines the key considerations in the deployment of network virtualisation in a mobile network environment. The topics covered within represent solutions to the potential obstacles mobile operators may face when wishing to capitalize on network virtualisation (covering both Network Functions Virtualisation and Software-Defined Networking).

It also provides an overview of the steps mobile operators should take to adopt this technology and where appropriate, provide an indication of what they will need to complete the work and which external organisations are best placed to deliver it. Finally, it outlines a number of examples and approaches that have been taken by operators to identify and address the gaps.

9.5 3GPP: TR 33.4848 v0.6.0 (2019-11) Study on Security Impacts of Virtualisation (DRAFT)

https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3574

The document considers the consequences of virtualisation on 3GPP architectures, in order to identify threats and subsequent security requirements. The document highlights 28 key security issues with virtualisation in 3GPP network functions and recommends a number of mitigations and solutions that reduce the overall risk. This document is still in draft, with the

most recent version made available on 29th of January 2021. Readers should look for the most recent version when consulting this document.

9.6 NIST: SP 800-125 Guide to Security for Full Virtualisation Technologies

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf

The purpose of the guide is to discuss the security concerns associated with full virtualization technologies for server and desktop virtualization, and to provide recommendations for addressing these concerns.

9.7 NIST: SP 800-125B Secure Virtual Network Configuration for VM Protection

SP 800-125B, Secure Virtual Network Configuration for VM Protection | CSRC (nist.gov)

The purpose of this NIST Special Publication (SP) is to provide an analysis of various virtual network configuration options for protection of virtual machines (VMs) and present recommendations based on the analysis. The relevant configuration areas discussed in this publication are network segmentation, network path redundancy, traffic control through firewalls, and VM traffic monitoring. Each configuration option in each of these areas has different advantages and disadvantages, which are identified in this publication. Analysis of these has led to the development of one or more security recommendations for each configuration area.

9.8 NIST Special Publication 800-190 Application Container Security Guide

Application Container Security Guide (nist.gov)

Application container technologies, also known as containers, are a form of operating system virtualization combined with application software packaging. Containers provide a portable, reusable, and automatable way to package and run applications. This publication explains the potential security concerns associated with the use of containers and provides recommendations for addressing these concerns.

9.9 ETSI: Industry Specification Group (ISG) Network Functions Virtualisation (NFV)

ETSI - NFV

ISG NFV has developed over 100 different specifications and reports for the virtualization of network functions, with focus on the management and orchestration of virtualized resources. From an architectural point of view, NFV specifications describe and specify virtualization requirements, NFV architecture framework, functional components and their interfaces, as well as the protocols and the APIs for these interfaces. Another set of NFV specifications define the structure and format of deployment templates and how to package all artefacts which are used by the NFV management and orchestration framework.

ISG NFV also studies VNF performance, reliability, and resiliency matters, analyses the security challenges linked to virtualization (trust, attestation, regulation) and specifies associated requirements. In support for 5G deployments, the ISG NFV specifications include support for multi-site and multi-domain deployments, as well as network slicing. New virtualization technologies such as support for containerized VNFs and container infrastructure management are tackled in studies and on-going normative specifications work. In addition, the ISG NFV specifies requirements for hardware acceleration, multi-tenancy, autonomous networks, etc.

Of particular note are:

NFV-SEC 003: Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance

NFV-SEC 006 Network Functions Virtualisation (NFV); Security Guide; Report on Security Aspects and Regulatory Concerns

NFV-SEC 014 Network Functions Virtualisation (NFV) Release 3; NFV Security; Security Specification for MANO Components and Reference points.