Security Challenges of Small Cell as a Service in Virtualised Mobile Edge Computing Environments

Vassilios Vassilakis[1], Emmanouil (Manos) Panaousis[2] and Haralambos Mouratidis[2]

[1]University of West London
[2]Secure and Dependable Software Systems (SenSe) Research Cluster
University of Brighton

University of Brighton

Some Info…

- Brighton is a seaside resort and the largest part of the city of Brighton and Hove situated on the south coast of England

- I am a Senior Lecturer with the University of Brighton, which is a UK university of over 21,000 students and 2,500 staff based on five campuses in Brighton, Eastbourne and Hastings on the south coast of England

- I am co-leading research on Cyber Security and Privacy

SESAME

- This work is funded by the H2020 ICT-14-2014 **SESAME** project, under the grand agreement 671596
- Targets innovations around three central elements in 5G
  - the placement of network intelligence and applications in the network edge
    - ✤ Network Functions Virtualisation (NFV)
      - ✓ NFV can be further enhanced with the concept of software-defined networking (SDN) decoupling the control plane from the data plane
    - ✤ Edge Cloud Computing
  - the substantial evolution of the **Small Cell concept** is already mainstream in 4G but expected to deliver its full potential in the challenging high dense 5G scenarios
  - consolidation of **multi-tenancy** in communications infrastructures, allowing **several operators/service providers** to engage in new sharing models of both **access capacity** and **edge computing** capabilities
- Small Cell as a Service, MEC, NFV, and SDN are going to be integral parts of 5G networks

Motivation

- Rapid advances in the industry of handheld devices and mobile applications has fuelled the penetration of interactive and ubiquitous web-based services into almost every aspect of our lives

- Users expect zero latency and infinite-capacity experience

- 5G technologies aim at addressing limitations of 4G to offer high speed and personalized services when and where is needed

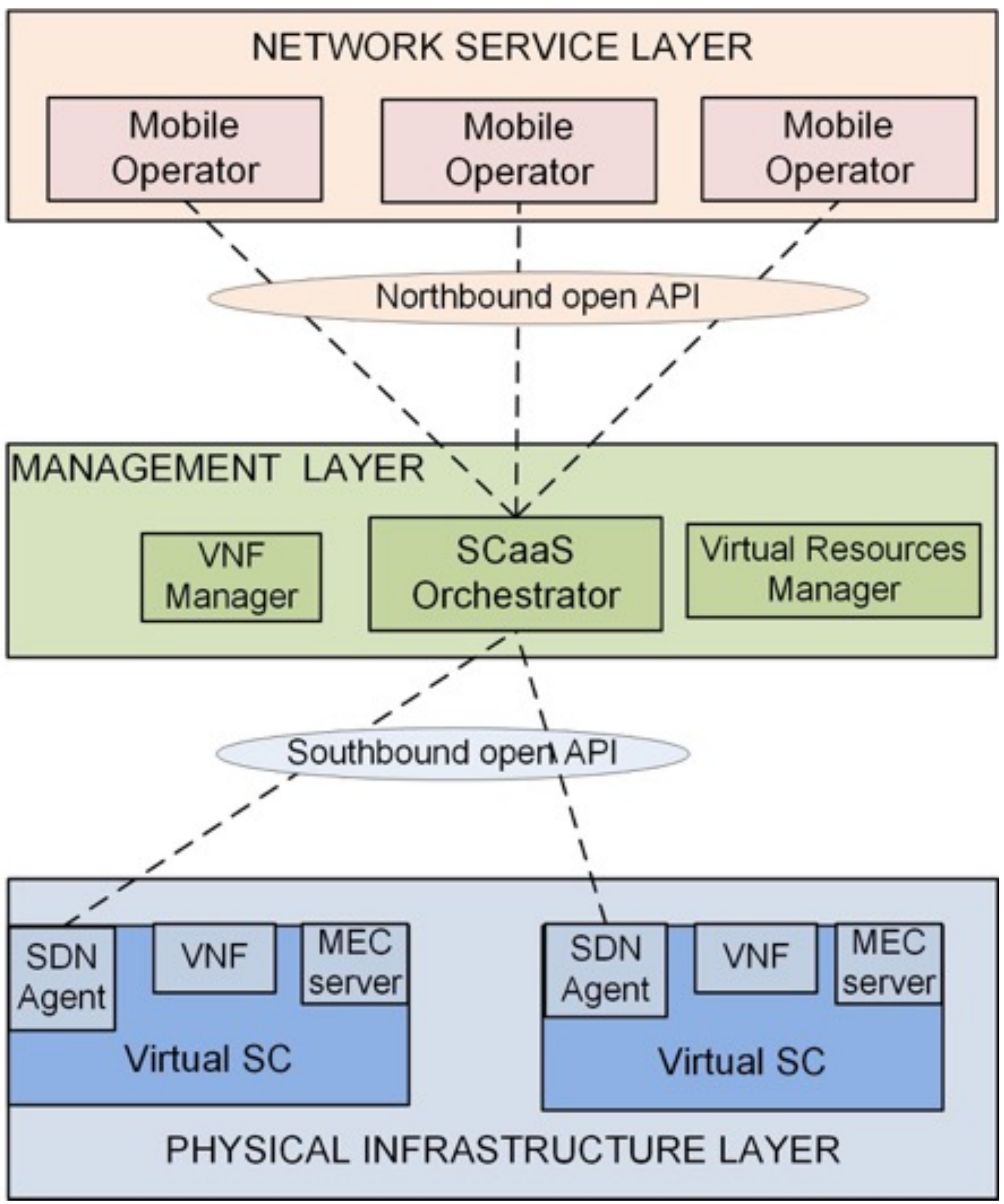
- Research on next-generation 5G wireless networks is currently attracting a lot of attention in both academia and industry

- 5G development and standardisation activities are still at their early stage

5G

- 5G systems are going to extensively rely on dense Small Cell (SC) deployments
  - exploit infrastructure and **Network Functions Virtualization** (NFV)
  - push the network intelligence towards network edges by embracing the concept of **Mobile Edge Computing** (MEC)
- The primary benefit that comes with **Small Cell as a Service** (SCaaS) is that **independent actors own** and **lease their cellular infrastructure to multiple mobile network operators** (MNOs)
- SCaaS provides a natural **multi-tenant support**, by allowing each MNO to be a tenant of the infrastructure and **getting a slice** of the physical SC infrastructure
- We can leverage SCaaS to provide **high-speed**, **low-latency** communications and to offload the mobile core network traffic and computation to the network edge, giving life to the concept of MEC

System architecture



- **Physical Infrastructure layer**
  - The physical SC is sliced into **virtual SCs** (VSCs)
  - To enable MEC services, each VSC is equipped with a **MEC server**, which has the ability to communicate with the Cloud and to execute functions
  - Each VSC accommodates a number of VNFs
- **Management layer**
  - Multiple MEC servers are clustered to provide enhanced services in the form of a **light data centre** managed by the **virtual resources manager** (VRM)
  - Each VSC is managed by the **SCaaS Orchestrator** via an **SDN agent**
- **Network Service layer**
  - Above the management layer there is the service layer, in which **multiple tenants** (i.e., MNOs) are accommodated
  - MNOs have **on-demand access** to SC resources **without owing** the physical infrastructure
  - MNOs communicate with the SCaaS Orchestrator, located in the management layer, who **orchestrates the allocation of virtual resources** to MNOs

Security

- Security will be a fundamental enabling factor of small cell as a service (SCaaS) in 5G networks
- We propose a set of **criteria** to facilitate a clear and effective taxonomy of security challenges of main elements of 5G networks
- We devised, in a high level manner, the most prominent threats and vulnerabilities against a broad range of targets at the intersection of SCaaS, NFV, and MEC
- These will have crucial effect on legal and regulatory frameworks as well as on decisions of businesses, governments, and end-users
- Our analysis aims to serve as a staring point towards the development of appropriate 5G security solutions

Security components

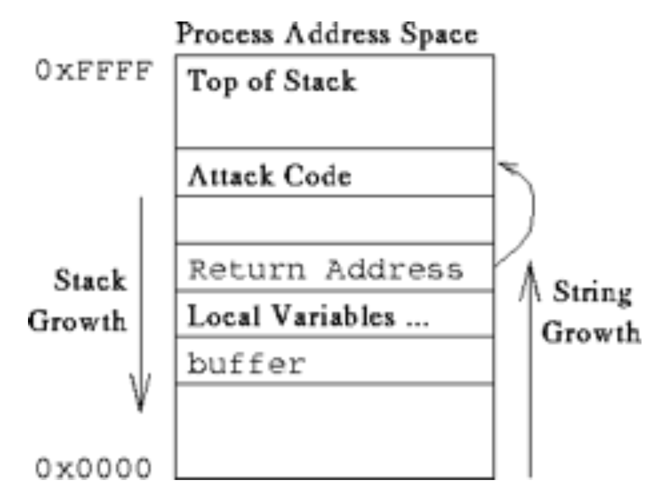
- Security challenges that arise due to specific architectural characteristics and interaction of various components and layers of SCaaS are based on
  - **Precondition**
    - ✤ What are the **necessary conditions** to be met before the adversary is able to launch the attack?
    - ✤ example: Adversary **has some particular access rights** that may use to escalate its access rights and compromise components
  - **Vulnerability**
    - ✤ What are the vulnerabilities of the system components or the network interfaces, which can be exploited by the adversary?
  - **Target**
    - ✤ Which components or interfaces are potential attack targets?
    - ✤ example: whether the attacker aims to compromise the control or the data plane or both
  - **Method**
    - ✤ What are the various attack methods, tools and techniques that the adversary might use?
    - ✤ Examine whether the adversary follows an active (e.g., replay attack) or passive strategy (e.g., passive reconnaissance)
  - **Effect**
    - ✤ What is the impact of a successful attack on the victimised system component or network interface? (e.g. unavailability of some services, financial costs, and leakage of sensitive data)

Precondition

- **Specific configuration**
  - To launch an attack against a component, the adversary requires that this component has specific **exploitable configuration** or **runs a specific software**
  - **example**: In SESAME, a precondition for a denial-of-service (DoS) attack can be a specific configuration of the VRM with regard to the **allocation of resources** to tenants
- **Ubiquitous connectivity**
  - If a network **component** or **function** can be accessed via the public Internet, this may be exploited by a **remote adversary** — Discovering vulnerable component and sending messages via control or data plane
  - example: In SESAME, SCaaS Orchestrator may be a distributed function with its instances located across multiple SCs (e.g. in the form of a VNF)
    - ✤ If public Internet is used to **remotely configure various SCaaS policies**, this can be exploited by the adversary
- **Privileged access**
  - The adversary has privileged access to some parts of the network components or functions
  - The privileged access can be either at the **administrator** or **user level**
  - **example**: The adversary may be legitimate UE (user equipment) receiving service from its MNO, with the latter being a legitimate tenant of the SC network infrastructure

Vulnerability

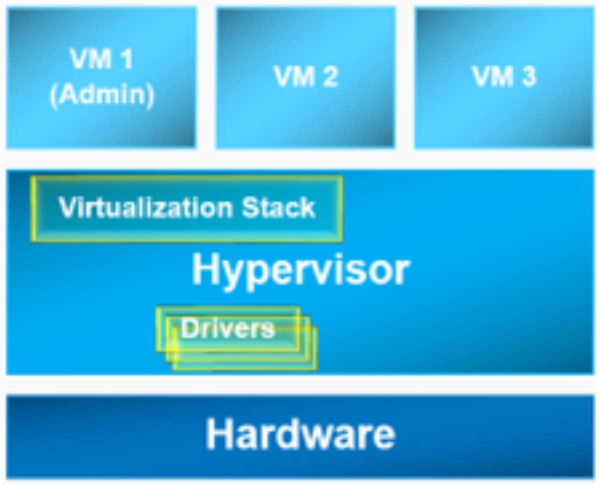
- **SDN controller weaknesses**
  - Some vulnerabilities are caused by flaws in software and programming errors
  - This may lead, for example, to control flow attacks and buffer overflow attacks
  - This issue is particularly important in the context of next-generation wireless networks, where the trend is to implement the control plane **in software** and to **virtualize network functions**
- **Flaws of NFV platforms**
  - **Flaws of the virtualisation platform**, may constitute the guest operating system (OS) vulnerable to side-channel attacks
- **Cloud based management**
  - Vulnerabilities stem from the Cloud based management nature of certain network components
  - **example**: The Cloud based interface used for configuration and updates could be used as a potential attack channel



Vulnerability

- **<u>Weak access control and authentication</u>**
  - Use of **weak or default passwords** could be easily exploited by an adversary
  - Components may have hard-coded passwords (**CWE-259: Use of Hard-coded Password**), which can be exploited by the adversary towards the establishment of backdoor access (stealthy or not)

- **<u>Weak cryptographic mechanisms</u>**
  - Weaknesses or improper use of cryptographic mechanisms may lead to security breaches in authentication processes and data confidentiality
  - **example**: Adopted public-key scheme that enables the encryption of the communications among SC, UE, and the Cloud, should be sufficiently secure
- **<u>Physical small cell infrastructure</u>**
  - Attacks on specific piece of hardware that is used in the cellular network
  - **example**: the physical SC infrastructure can be a target of hardware attacks



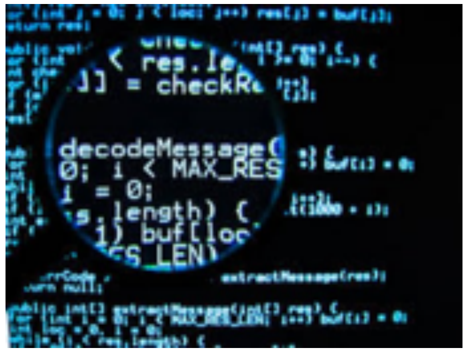
- **<u>NFV-based management system</u>**
  - Some attacks initiated inside virtualised environments may aim at taking control of the **Hypervisor**
  - The **SCaaS Orchestrator** and **VNF Manager** are attractive attack targets due to being in the ' middle of the system model architecture
  - **Impersonation** by the adversary of **one of the VNFs** or the **MEC server** when communicating with the management layer is also a threat

Target

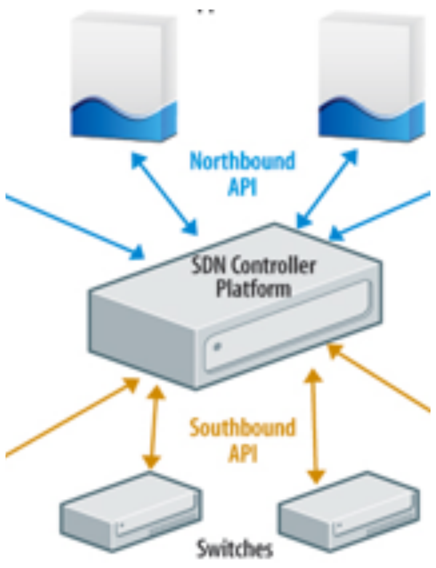
- **VM-hosted operating system**
  - Both host and guest OS may be targeted
  - The adversary could attempt to break the isolation (guest virtual machines (VMs), host and guest VMs) by exploiting flaws of the virtualisation platform in use
- **MEC-based application**
  - A **certain application that runs on a MEC server** is a potential attack target
  - Due to clustering of MEC servers into the Light DC and their communication with the Cloud, a **MEC server** is a target that can be used as a door to attack other network entities and components
- **Protocols**
  - A usual attack target is the protocol used for communication, management or control purposes, such as the MobileFlow protocol
  - **Southbound** and **northbound interfaces** are potential attack targets when attempting to hijack the communication of the SCaaS Orchestrator with VSCs and MNOs
  - Possible attack targets are
    - communication of the **VNF Manager with VNFs** in a SC;
    - communication of the **VRM with MEC servers**
  - **example**: This may enable an adversary to alter the network policies and create attack channels

Method

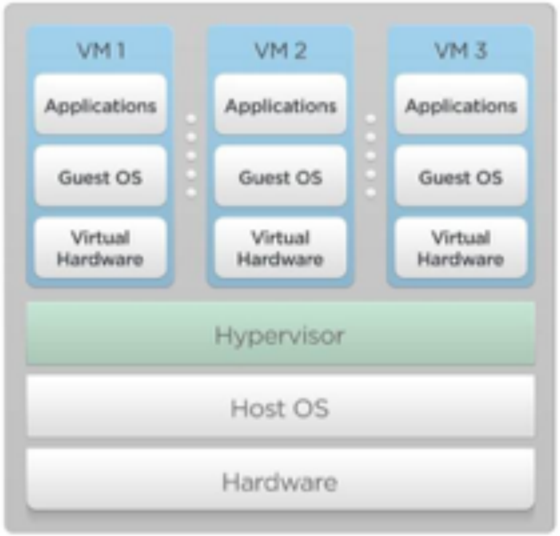
- **<u>Reverse engineering</u>**
  - The adversary collects and analyses sensitive information about the network and its functionality
  - This may enable the adversary to identify vulnerabilities in the software or network interfaces
  - The adversary may exploit weaknesses in the implemented access control mechanisms and exploit a device through normal usage, i.e., as a legitimate user



- **<u>SDN controller hijacking</u>**
  - By exploiting SDN controller's implementation weaknesses, the adversary tries to **divert the control flows to a controlled device**
  - The captured messages can be discarded or manipulated **preventing the data plane entities from proper operation**

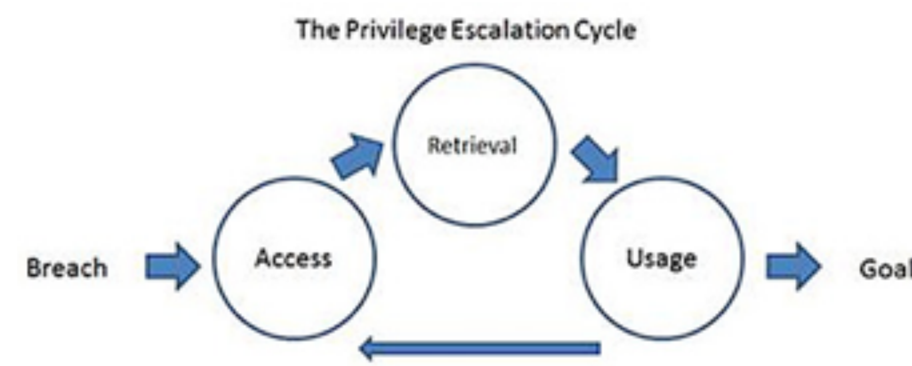


- **<u>VNF/VM infection</u>**
  - The adversary infects a virtual network component (e.g. VNF) with malicious code
  - In a typical virtualised environment, guest VMs are expected to run in complete isolation, enforced by the Hypervisor
  - However, such virtualised environments may be vulnerable to the so-called VM escape attack
    - a process of breaking out the aforementioned VM isolation, e.g. by installing malware on the Hypervisor



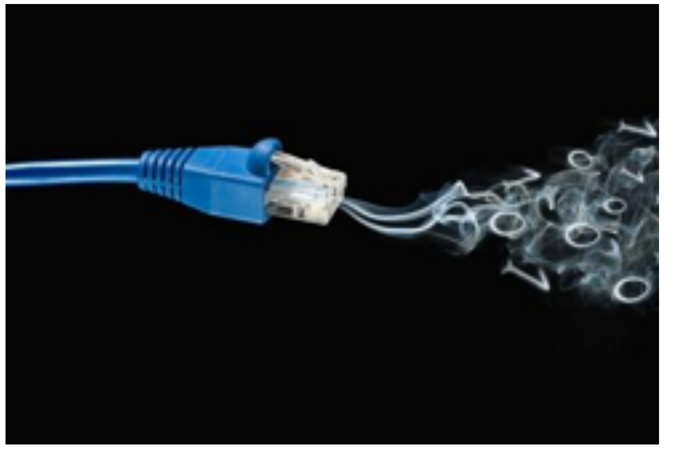
Effect

- **<u>VM/VNF privilege escalation</u>**
  - The adversary, who has already some level of limited access privilege (e.g. to a VM or a VNF), manages to gain more privilege
- **<u>Denial of service</u>**
  - A potential outcome of attacks can be DoS leading to
    - switched off or malfunctioning SC, or
    - unavailable MEC servers
  - DoS against SCaaS Orchestrator can cause **service disruption** and **data loss**
  - In a multi-tenant environment, security implications that may arise due weak isolation between tenants may allow adversaries to launch DoS from within the SC after compromising a tenant
- **<u>Tenant data integrity violation</u>**
  - Particularly important issue in a virtualised multi-tenant environment as some tenants may be malicious
  - Some data or code, including various configuration settings and security policies, can be altered



Effect

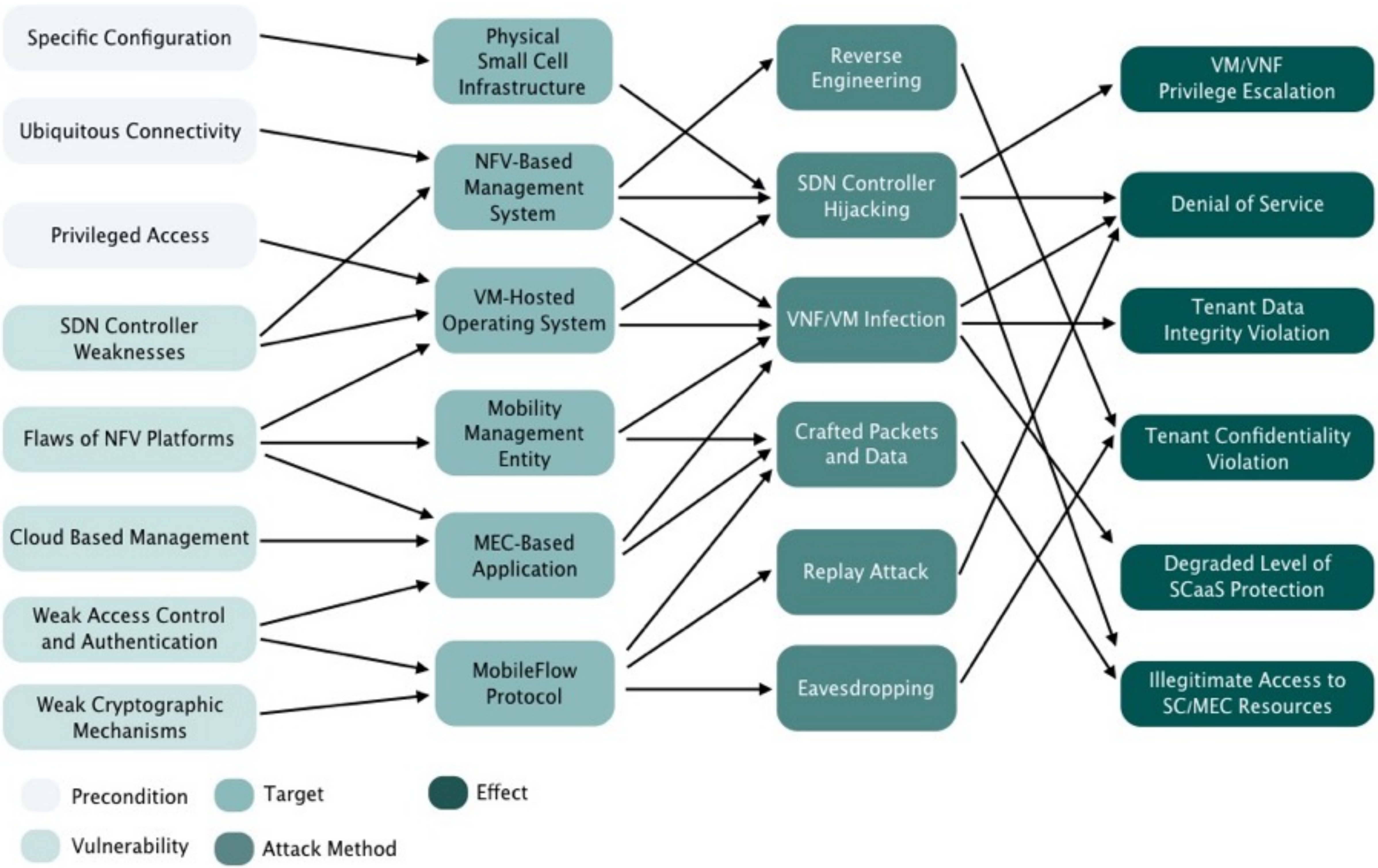
- **<u>Tenant confidentiality violation</u>**
  - Sensitive information of a tenant may be leaked and made available to the adversary or to a malicious tenant



- **<u>Degraded level of SCaaS protection</u>**
  - A possible effect can be the overall degradation of SCaaS infrastructure protection
  - Achieved, for example, by **altering the security policies** or **switching to weaker cryptographic mechanisms**

- **<u>Illegitimate access to SC/MEC resources</u>**
  - The adversary gains illegitimate access to the SC resources (physical or virtual) or MEC environment

Dependencies



Example

- **Aim**: DoS
- **Attack method**: VM/VNF infection by injecting malware to:
  - **Targets**:
    - the management system (e.g. to the VRM or the VNF Manager)
    - a VM-hosted OS, or
    - a MEC-based application (i.e., by compromising a MEC server)
- To target, e.g., the VM-hosted OS, the adversary may exploit:
  - **Weaknesses**: the SDN controller weaknesses or flaws of NFV platforms
  - **Preconditions**: take advantage of any privileged access rights

Conclusions

- Can 5G security be a carbon copy of 4G security?
    - If 5G had only been about bitrates, for example, the answer would likely be yes.
- 3GPP's approaches for 3G and 4G – which brought the industry highly secure radio and core network protocols, subscriber authentication and more are largely still valid
- There must also be new considerations for 5G security design
- In future work, we intend to study and evaluate prominent security solutions developed for **protecting virtualised SC networks** and systems per se, focusing on NFV, SDN, and MEC

Thank you for your attention!

Questions?