IoRL Deliverable D2.4

Threats Analysis and Integrated Security Framework for the IoRL Use Cases

Editors:	Krzysztof Cabaj, Warsaw University of Technology Wojciech Mazurczyk, Warsaw University of Technology
Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Contractual delivery date:	31st May 2018
Actual delivery date:	
Suggested readers:	Participants of the EU projects related to SDN, and security in 4G/5G networks Consumer Product OEMs such as Samsung, Huawei, Nokia
Version:	1.0
Total number of pages:	49
Keywords:	5G Networks Security, Integrated Security Framework, Information Security

Abstract

In this report first, the threat analysis for the IoRL system and the specific use cases it is applied to are assessed. Based on the obtained results an Integrated Security Framework (ISF) is introduced as a countermeasure and its architecture is described in details.

Disclaimer

The research leading to these results has received funding from the European Union Horizon 2020 Programme under grant agreement number 761992 — IoRL — H2020-ICT-2016-2017/H2020-ICT-2016-2.

Impressum

Internet of Radio Light (IoRL)

WP2 Usage Scenarios, Requirement Specifics and System Design

Task 2.6: Threats Analysis and Integrated Security Framework

Editors: Krzysztof Cabaj, Wojciech Mazurczyk, Warsaw University of Technology

Work-package leader: Moshe Ran, MostlyTek

Estimation of human resources invested in the Deliverable

BRUNNEL= 0.45 PM

MTEK = 1 PM

WUT = 2,5 PM

Executive summary

Nowadays, cybersecurity is one of the most important aspect that has to be considered for every new networking system that is created. Furthermore, security is not something that can just be retrofitted to a solution, it is an essential aspect that needs to be considered from the inception. This is the state of the art practice followed across the industry and is called “security by design”, whereby concepts and solutions are critically reviewed and analysed from early on to detect threats and vulnerabilities and include and design in mitigation.

IoRL follows this practice and we present in this document the main security challenges for the Internet of Radio Light (IoRL) system, and based on our analysis we propose appropriate countermeasures.

First, we start with an in-depth security analysis of each technology and components involved within the IoRL system architecture. The following groups of threats for the IoRL solution have been identified:

- IoRL end user devices-related threats (user-specific) where examples include e.g. Man-in-the-Middle (MitM) attacks performed by malicious users in order to influence legitimate IoRL users or their devices in order to capture their sensitive data (like credentials), to tamper with the legitimate users’ communication (in order to impersonate them) or to disrupt it via Distributed Denial of Service (DDoS) attacks.
- IoRL infrastructure-related threats (component-specific) which include attacks on crucial points of the IoRL architecture in order to overload or impersonate them e.g. by performing DDoS attacks on the SDN or RRLH controllers or eavesdropping and then spoofing their communication. It is also worth noting that these types of attacks can be launched by malicious IoRL users (inside threat) or by remote attackers (remote threat) residing somewhere in the Internet or in the vicinity of the IoRL system components, for example, mmW or VLC receivers and/or transmitters.
- IoRL-related threats (architecture-specific): such attacks can be possible or could be amplified because of the heterogeneous nature of the proposed system involving coexistence and integration of various networking technologies. Due to this fact some unexpected interactions or vulnerabilities can be discovered.

Considering the above we analysed both the IoRL architecture as well as the defined specific use cases, namely train station, museum, smart home and supermarket scenarios, from the specific perspective of security in detail. Based on our findings an Integrated Security Framework (ISF) have been designed and will be developed within the IoRL project in order to mitigate these threats and provide an adequate level of security. While designing ISF we have also utilized experiences and analysed solutions from the existing finished or ongoing 5G security projects and standardization activities. A key, fundamental technology used within the IoRL ISF is SDN that provides important security features like security monitoring and management and draws on the results of completed and still ongoing 5G PPP projects. Finally, we depict some exemplary scenarios to demonstrate how the IoRL ISF can be efficiently used to counter selected threats.

List of authors

Company	Author	Contribution
Warsaw University of Technology	Krzysztof Cabaj, Wojciech Mazurczyk, Piotr Nowakowski, Piotr Żórawski	Coordination of the deliverable contributions from partners and their integration, D2.4 structure contribution to majority of the sections.
Brunel University	John Cosmas, Nawar Jawad, Ben Meunier, Kareem Ali, Hongying Meng	Chapter 2, Chapter 3, Chapter 5
MostlyTek Ltd	Moshe Ran, Einat Ran	Editorial, Sections 1.3, 2.3, 3.2

Table of Contents

List of figures

List of tables

Abbreviations

5G	Fifth Generation (mobile/cellular networks)
5G PPP	5G Infrastructure Public Private Partnership
AES	Advanced Encryption Standard
AP	Access Point
CHDCS	Cloud Home Data Center Server
C&C	Command & Control
DoS	Denial of Service
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
ENISA	European Union Agency for Network and Information Security
FTP	File Transport Protocol
GNSS	Global Navigation Satellite System
GTP	GPRS Tunneling Protocol
HTML	Hypertext Markup Language
ICMP	Internet Control Message Protocol
IoRL	Internet of Radio Light (project)
IP	Internet Protocol
ISF	Integrated Security Framework
LAN	Local Area Network
LOS	Line of Sight
MAC	Medium Access Control
MIB	Master Information Block
MitM	Man-in-the-Middle
MCC	Mobile Cloud Computing
mmW	mmWave
NFV	Network Function Virtualization
NLOS	Non-Line-Of-Sight
OFDM	Orthogonal Frequency-Division Multiplexing
PBCH	Physical Broadcast Channel
PDCP	Packet Data Convergence Protocol
PPP	Poisson Point Process
PSS	Primary Synchronization Signal
RRLH	Remote Radio Light Head
RAN	Radio Access Network
SAMS	Security Analysis & Mitigation Service
SDN	Software Defined Network
SDR	Software Defined Radio
SIB	System Information Block
SNR	Signal-to-Noise Ratio
SRS	Sounding Reference Signal
SSC	Smart Shopping Car
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security

UC	Use Case
UDP	User Datagram Protocol
uRLLC	Ultra-Reliable Low-Latency Communications
vIDS	virtualised Intrusion Detection System
VF	Virtual function
vFW	virtualized Firewall
VLC	Visible Light Communications
VSF	Virtual Security Function
WLAN	Wireless Local Area Network

1 Introduction

1.1 Objective of this document

The main objectives of this document are to:

- Describe the main threats specific to the IoRL system architecture.
- Describe the threats analysis for the use cases defined for IoRL.
- Describe the details of IoRL Integrated Security Framework.
- Describe the Integrated Security Framework Demonstrator Selected Scenarios.

1.2 Structure of this document

The rest of the document is organized as follows:

- Section 2 describes the classification of main network threats as well as most notable examples are described there in detail,
- Section 3 presents an analysis of the specific threats which are characteristic for the IoRL system,
- Section 4 focuses on the security analysis of the use cases considered within IoRL project,
- Section 5 outlines the architecture of the proposed Integrated Security Framework (ISF) which is considered as a main countermeasure against the identified threats,
- Section 6 presents some exemplary scenarios how ISF perform under different attack conditions.

1.3 Relation to other 5G security projects and standardization activities

While designing IoRL Integrated Security Framework (described in detail in Section 5) we took inspirations from the previous 5G security related projects completed or ongoing under Horizon 2020 programme. This subsection summarizes these relationships.

As mentioned the main issue addressed within IoRL from the 5G Security perspective is the threats analysis and development of the integrated security framework for the use cases defined within the project (i.e. smart home, museum, train station and supermarket). IoRL project integrates various networking technologies (WLAN, eNB/HeNB, mmW, VLC and SDNs) and each of them have a specific set of characteristic features and potential security threats and vulnerabilities that still are often not completely resolved and still need addressing. For such a heterogeneous network a careful threat analysis will be performed in order to identify most important security hazards. Based on this analysis the dedicated security framework is devised that will provide secure communication and preserve users' privacy. Most importantly it will address attacks that could be possible or could be amplified because of the mentioned network technologies integration and coexistence. The proposed security framework will be an integral part of the developed architecture following security-by-design rule.

As mentioned in the literature and industry reports [1, 2] 5G will be mainly affected by technologies allowing softwarization of networking functions which will be achieved with Software Defined Networking (SDN) and Network Function Virtualization (NFV). This also

pertains to providing security aspects for 5G network, however, in order to achieve this a number of challenges and issues (also security-related) need to be addressed.

5G Security Requirements defined in [1] list several most important aspects of security for 5G networks. Among them security monitoring, management and automation are the most vital from the IoRL perspective. This is crucial to be able to deal with the current threats we know from the communication networks but also with the new threats caused by evolution of networks to 5G and technologies involved. Thus, it is vital to include security monitoring by design and to enable security monitoring during the 5G network infrastructure operations to proactively identify and efficiently react to security threats and provide mitigation solutions. From this perspective, effective and efficient security monitoring and management system, which is able to discover evidence of potential threats in a nearly real-time manner is one of the key components to provide the necessary trust and confidence of various stakeholders to fully release the potential of 5G networks.

Therefore, considering above, the design and implementation of the security monitoring and management system for IoRL will be based on SDN and NFV as it is agreed that it is most favorable approach for this challenge [1, 2]. Moreover, the proposed integrated security function will be tailored to the requirements of the IoRL use cases. Based on the SDN controller, a centralized system for security monitoring and manageability, providing near real-time awareness of network incidents status and effective enforcement of security policy will be designed and developed. To this purpose security-related VNFs will be created that will perform various security functions. Such a solution will also work effectively by enabling correlation, aggregation and analysis of the security-related data originating from different sources in order to provide a complete network-wide view of the security posture (security analytics).

From the 5G PPP Phase 1 projects, the project CHARISMA [3] was proposing a similar approach as it relied on a real-time, automated Security Management Framework for 5G telecommunications networking. It was focused on implementing a continuous and closed loop real-time environment inspection regime, based on analytics, policy-based decisions and actuation/enforcement via cloud and SDN orchestration procedures. In particular, the virtualized nature of 5G networking itself allows the automated instantiation, deployment, configuration and management of Virtual Security Functions (VSFs) in real time, with a centralized orchestration approach. CHARISMA implements two security-related VNFs: a virtualised Intrusion Detection System (vIDS) equipped with advanced traffic analysis and monitoring capabilities for attack detection; and a virtualized firewall (vFW) able to filter the passing traffic based on a predetermined set of security rules.

The SELFNET project was developing a Self-Protection use case [4] where typical Network Intrusion Detection Systems (NIDS) are used by leveraging these techniques and virtual functions. The SELFNET approach is related closely with the CHARISMA approach, however it proposes a two-loop innovation to reduce the amount of VNFs inserted along the data path in order to reduce delays and overheads and simultaneously to enable distributed sensing of key metrics that can be utilized for the detection phase of the threats. SELFNET is also proposing an innovative security management where the deployment of VNFs is localized just in the position along the data plane where it is more appropriate to detect and eliminate potential attacks.

Finally, the VirtuWind project [5] brings two novel elements to the SDN controller: Reference Monitor and Security Manager. The former coordinates the component sequence of operations and verifies all entity operations/requests against the specified access control policies. The latter i.e. Security Manager authenticates involved entities, keeps track of security-related activities for accounting purposes and communicates pertinent data to the backend e.g. for more sophisticated analysis techniques.

While designing Integrated Security Framework for IoRL system, which is the "heart" of the security we rely on the previous experiences and research developments of the 5G PPP Phase 1 projects mentioned above i.e. CHARISMA, SELFNET, and VirtuWind.

Standardization activities on 5G security are summarized in the table below.

Table 1-1: Standardization activities on 5G security

Standardization body	**URL**	**Activities**
3GPPP SA3	http://www.3gpp.org/specifications-groups/sa-plenary/sa3-security	Threat analysis, Requirements on security, Security architecture and protocol specifications Definition of 17 security domains(Architecture, Authentication, RAN security, Key Management, etc.)
ETSI ISG NFV	http://www.etsi.org/technologies-clusters/technologies/nfv	Security monitoring & administration for NFV Security assessment for NFV platform etc.
GSMA	www.gsma.com	5G trust models etc.
NGMN	https://www.ngmn.org	Security requirements as DoS protection, Network Slicing, 5G Multi access Edge Computing (MEC)
Others	IETF Open Network Foundation	5G IP, Netslicing SDN related security

2 Network/system Threats Classification

2.1 Active/passive network/system attacks classification

In the literature there exists many potential ways to classify network/system attacks. One of the most well-known classification is related to how the attacker can affect the passing network traffic or system resources. Such classification is presented in the Figure 1. If the attack attempts to learn or make use of information from the passing network traffic or system but does not affect the transferred data or system resources then it is called a *passive attack*. Alternatively, an *active attack* relies on altering the traffic flows/system resources or affect their operation.

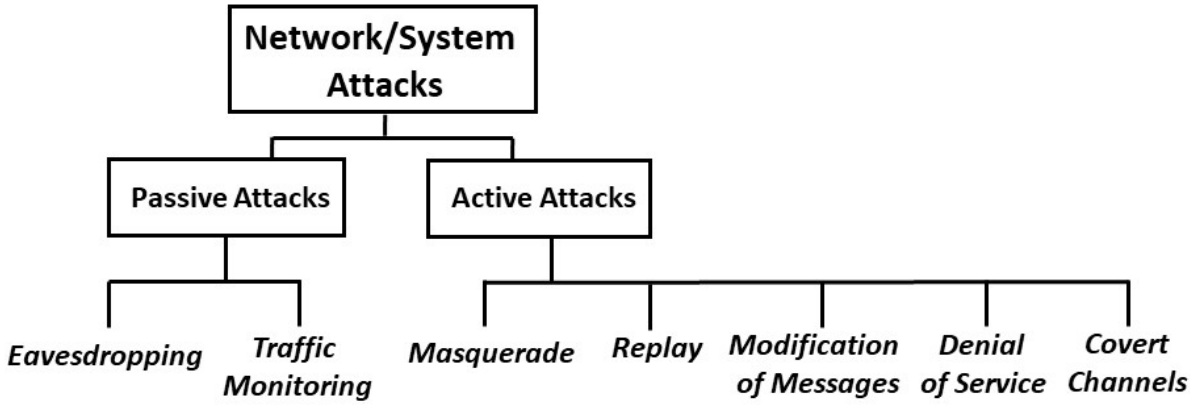

Figure 1 – Network/system attacks classification

Typically, ***passive attacks*** focus on eavesdropping or on monitoring of transmissions happening in the network/system. The main aim of the attacker is to obtain information that is being transmitted e.g. login credentials, specifics of the network protocols used, etc. Such type of attack is quite hard to detect as the attacker is not actively affecting any target machine or participating in network traffic exchange so there is no direct alteration of the data. Usually, the transmitted and received network traffic appears as a typical legitimate one and neither the sender nor the receiver is aware that a third party has potentially read the messages or observed the traffic patterns. The potential prevention against passive attacks include encryption of the passing network traffic or system communication.

Another aspect of eavesdropping is the capability to intercept the transmitted signals based on improving the link budget through expensive and sensitive interception channels.

- Key issues to consider for eavesdropper regarding the channel model are:
  1. In the 60GHz frequency band Path Loss (PL) of interceptor has significantly larger propagation loss according the Friis transmission equation, in case of line-of-sight (LOS), than the legitimate receiver. As a consequence, high directional receive antennas have to be used to compensate for the larger propagation loss to sustain operation over typical WLAN distances of up to several tens of meters. Hence, interceptor's channel model should take into account spatial (angular) coordinates of the channel rays at the receive sides
  2. For the legitimate receiver, most of the transmission power is propagated between the transmitter and the receiver through LOS and low-order reflected paths. However, interceptor needs in order to establish an interception-link, to

use steerable directional antennas have to be pointed along the LOS path (if available) or to use one of the reflected paths.

3. As demonstrated by experimental investigations [6], each reflected path actually consists of a number of rays closely spaced to each other in the time and angular domains due to fine structure of the reflecting surfaces. Hence, interceptor needs to apply sophisticated clustering approach, with each cluster corresponding to the LOS or Non-Line-Of-Sight (NLOS) reflected path.
4. VLC interception consideration: as indicated by [7] and [8] VLC-based communications can be eavesdropped by outside observer, although VLC does not go through solid objects like walls. VLC signals can be intercepted through windows or small gap under the door. Additionally, eavesdropper located in the same room without LOS to VLC Tx can benefit from reflections on the walls.

- Key parameters for Traffic Monitoring consideration:
  Here the interceptor aims at finding key metadata parameters such as size, origin, destination, frame timing etc.

Active attacks present the opposite characteristics when compared with passive attacks. In active attacks, an attacker is actively launching an attack against the target machines thus they involve some kind of modification of the data messages or the creation of false ones. In active attack the malicious party is actively sending traffic that can be detected.

Active attacks are usually divided into five groups of threats which include: masquerade, replay, modification of the messages, Denial of Service (DoS), and covert channel attacks.

Masquerade attack happens when the attacker tries to pose as another legitimate entity.

Replay attack includes reusing previously captured information from the passing network traffic and its subsequent retransmission to produce an unauthorized effect.

Modification of messages attacks are based on alteration of some portion of the legitimate message or their reordering or adding intentional delays to produce an unauthorized effect.

On the other hand, Denial of Service (DoS) attacks prevent legitimate users to access certain resources, service, machine or part of the network by temporarily or indefinitely disrupting them. Such attacks are typically accomplished by flooding the targeted machine/service/resource/system with exceeding network traffic or by targeting certain vulnerabilities within application/service/protocol in order to overload it and cause a not easily predictable event e.g. system/machine crash. If there is only a single source of attack we call it Denial of Service, otherwise when there are a lot of different sources of malicious traffic then it is called a Distributed Denial of Service (DDoS). The latter is more difficult to eliminate as such attacks cannot be mitigated by simply blocking/blacklisting a single source.

Finally, covert channels are created within legitimate network traffic using e.g. network steganographic techniques and they can be used, for example, to enable communication between an infected host and C&C (Command & Control) server operated by the attacker or to allow confidential data exfiltration.

Typical measures against active attacks include defensive systems like firewalls or ID/PS (Intrusion Detection/Prevention Systems). However, in general, it is hard to eliminate active attacks absolutely because of the wide variety of potential physical, software and network vulnerabilities. Instead, the main aim is to detect the presence of such attacks, block them and then to recover from any disruption or delays caused by them.

Below we describe in detail several chosen examples of the most popular and relevant network/system attacks that represent both passive and active attacks and which are important also from the IoRL security point of view.

2.2 Network Reconnaissance (Scanning Activity)

Reconnaissance is the activity performed by an intruder attempting to gather as much information about the targeted system as possible, in order to identify the vulnerabilities and potential weak points, which could be used later to launch attacks aimed to that system.

There are various methods to perform the network reconnaissance, including eavesdropping on the network and using probing techniques.

A probe (also called scanning) is a technique utilized by an intruder to gain information about the reachable hosts within the targeted network, and also about the applications running on the top of these hosts, which could be connected to a certain weak point which could be exploited later to perform a successful attack.

The type of information that could be gathered using various types of probes activities include, among others:

- using ICMP Echo Request/ Echo Reply technique used to test network hosts liveness probing that could reveal MAC and IP address of a probed host, while
- TCP/UDP scan technique which could be used for port enumeration to identify the TCP/UDP services running on the targeted host.
- Other types of probing can be used to find out about the operating system, versions and other applications running on that host.

The gathered information about the system from probing attempts can serve the purpose of the intruder to reveal system vulnerabilities, which then can be exploited later in a well-planned attack.

The following list describes the type of information which can be gathered during the reconnaissance activity:

1. Host liveness within the targeted network
    a. Getting its MAC address
    b. Getting it IP address
2. Port addresses
    c. Services running using the identified port addresses
3. Operating systems and applications running on the targeted hosts
    d. Including the versions of these applications

Apart from those mentioned above we can distinguish the following types of port scanning:

- Vanilla TCP connect () scanning

  The scanner attempts to connect to all ports (65,536). The connect () system call is designed using an OS in order to have the ability to open a connection with all available ports on the machine as connect () will be successful when the port is listening otherwise, the port will be defined as unavailable. No special privileges are needed or fast operation are needed making it a beneficial technique. The scan can be hastened using many sockets in parallel as having a separate connect () call for all the targeted ports in linear will consume much time. Finally, using non-blocking I/O

will give us the opportunity to watch all sockets at the same time and set a low time-out period.

- TCP Strobe Scanning

  An attempt to connect to only selected ports (typically, under 20) to known services to exploit a strobe does a narrower scan, only looking for those services the attacker knows how to exploit. It is just the modified version of the above category with more intelligent efforts.

- TCP SYN (Half Open) Scanning

  This is the half open technique, because the TCP connection is not complete at the stage. As known, a handshake is needed for TCP connection to be established as it sends a SYN request and waits for a SYN + ACK. So, because it is not a complete process the server process is never informed by the TCP layer because the connection is not complete. The primary advantage of this scanning technique is that fewer sites will log it. Unfortunately, root privileges are needed in order to build such custom SYN packets.

- TCP FIN (Stealth) Scanning

  It employs a couple of techniques for scanning the blocks, from the computer byrecording the port scan activities. One technique sends erroneous packs at a port and expecting that open listening ports will send back different error messages than closed ports. FIN packets are sent from the scanner to every port, according to the TCP/IP nature the closed ports reply using the proper RST while on the other hand the open ports ignore the FIN packets sent in question and close a connection. However, some systems are broken in this regard, but they send RSTs regardless the state of the ports making them not vulnerable to this type of scan. This scan is counted to be not very effective since some packets can be dropped or blocked on the wire or by the firewall consecutively.

- SYN/FIN Scanning using IP fragments packets

  The scanner sends packet fragments that can get through simple packet filters in a firewall instead of sending the searching packets to the port. As it splits the TCP header into IP fragments this can help to bypass some packet filter firewalls as they are not able to observe a complete TCP header that in the other case could match their filter rules. Some firewalls and packet filters queue all the IP fragments, but many networks ignore this queue due to the loss of performance caused by queuing.

- TCP FTP Proxy (Bounce Attack) Scanning

  The scanner goes through the FTP server in order to disguise the source of the scan (attacker's location). This technique is similar to IP spoofing in that it hides where the attacker comes from. It is very important to attackers to hide their tracks. FTP bounce scanning takes advantage of a vulnerability of the FTP protocol itself. The advantages of this approach are obvious (potential to bypass firewall, harder to trace). The main disadvantages are that this scan is slow, and that many FTP server implementations have finally disabled the proxy feature.

- UDP recvfrom () Scanning

  Port scanning usually means scanning for TCP ports, which are connection-oriented and thus it gives a wholesome feedback to the attacker. So, the scanner looks for open UDP ports, which are connectionless. In order for the attacker to find UDP ports, the attacker will send an empty UDP datagrams and if the port is listening, it should ignore the incoming datagrams or send back an error message. If the port is not listening (closed), the OS (operating system) would send back an ICMP Port unreachable message and there the attacker would find out if a port is not open by excluding the closed ports.

- ICMP Echo Scanning (Ping-Sweep)

  ICMP does not have a port abstraction so it is not a port scanning. But it is sometimes useful to determine what hosts in a network are up by pinging them all. ICMP scanning can be done in parallel, so it can be quite fast.

2.3 Denial of Service Attacks

Denial of service (DoS) is an attack on a computer network in which a user is destitute of the services provided on the server. This kind of attack focuses on the server, as it disrupts its operations e.g. by flooding the server with requests or false messages. The goal of this attack is to shut down the server. As shown in Figure 2, typically the attacker machine uses compromised machines (slaves) to flood the targeted server with false requests to disrupt its service to legitimate requests.

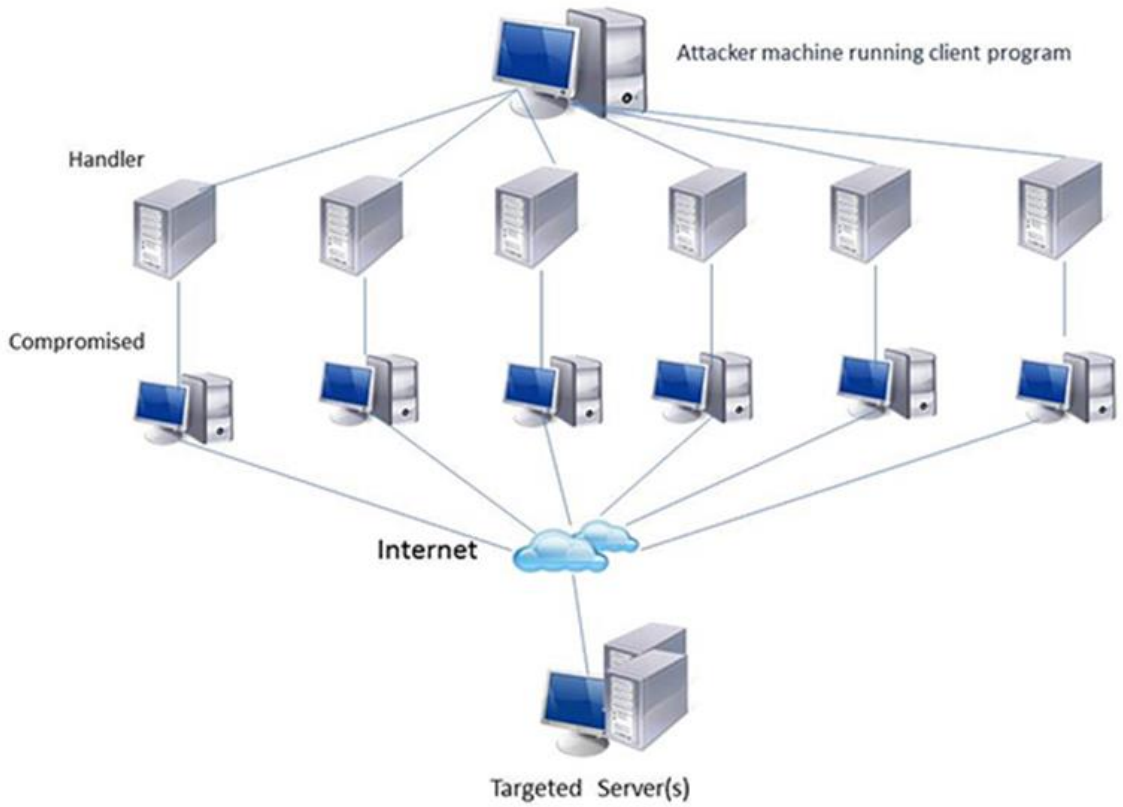

Figure 2 – A conceptual diagram of a DDoS attack

There is a different nature of attacks, where DDoS may be a part of a larger attack and they can be implemented by any of the following methods:

- Attempt to disrupt service to a specific person or a system.
- Attempt to disrupt connections between two machines, preventing access to a service.
- Attempt to prevent a specific user from accessing the service.
- Attempt to flood the network, thereby preventing legitimate network traffic.

The main types of Denial of Service Attacks include:

- Flooding / Bandwidth Attack
- Buffer Overflow/Ping of Death Attack
- Email Flooding Attack
- SYN Flooding Attack
- Teardrop Attack
- Smurfing / Smurf Attack
- Distributed DoS (DDoS)/ Botnet attacks.

2.4 Spoofing

The term spoof means to "fool", this happens on the Internet from people and programs that fool others through the process of impersonating and cheating others, as they get authorized in order to gain access to software and personal information. Spoofing is when a person or program masks his identity to represent as another (victim) by falsifying information to gain an illegitimate advantage on the behalf of the victims name.

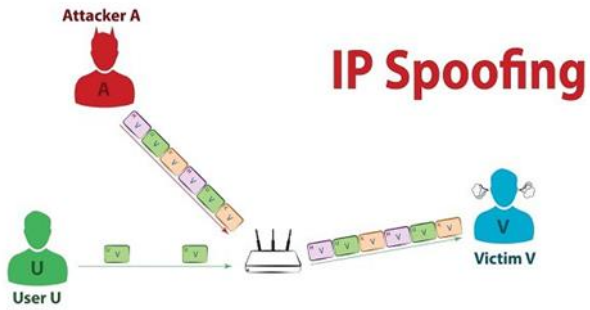

Figure 3 – IP Spoofing

There are several different types of Spoofing: PHY Spoofing, IP Spoofing, Email Spoofing and Network Spoofing.

5G NR 3GPPP rel-15 Jamming and Spoofing and Sniffing Vulnerability:

A valuable analysis 5G NR PHY layer Jamming, Spoofing and Sniffing assessment is provided in [9]. Its final conclusion is that compared to LTE, 5G NR 3GPP according to Release 15 is far less vulnerable to jamming, mainly because of its dynamic nature and removal of sparse control channels like the PCFICH.

It was concluded that the Primary Synchronization Signal (PSS) and Physical Broadcast Channel (PBCH) are the weakest subsystems. A jammer who transmits several fake PSS's signals can eventually cause denial of service (DoS) at the receiver.

Similarly, by jamming the PBCH signal, UE's will not be able to access critical information needed to connect to a cell.

Another aspect related to 5G NR jamming is the fact that the option of working in 60 GHz alone compared to the 24 GHz improves the resilience to jamming.

PHY-Layer spoofing: there are several types of PHY layer spoofing

Global Navigation Satellite System (GNSS) spoofing: GNSS is an umbrella of satellites that includes the US navigation system GPS, the other satellite navigation systems, such as the Russian GLONASS, the EU Galileo (expected to be fully operational by 2020) and China's Beidou.

- Key drawbacks of commercial stand-alone GNSS receivers are that are based on S/W defined radio (SDR) combined with low cost omni-directional antennas that are easy to deceive.
- The attacker deceives a GNSS receiver by broadcasting incorrect GNSS signals, structured to resemble a set of normal GNSS signals, or by rebroadcasting genuine signals captured elsewhere or at a different time. The spoofed signals may be modified to cause the receiver to estimate its position to be somewhere other than where it actually is, or to be located where it is but at a different time.

There are three main ways of spoofing IP addresses

- **Non-Blind Spoofing:** This type of attack is done when both the victim and the attacker share the same subnet, which helps to gain easy access of the other IP addresses.
- **Blind Spoofing**: This type of attack is done when both the victim and the attacker share the different subnet, which is a lot harder than a non-blind attack because the IP address is unreachable, however access can be still gained by sending packets to the victim's computer.
- **Man-in-the-Middle (MitM)**: This type of attack (spoofing) happens between two legitimate parties are communicating. The attacker would intercept their communication allowing himself control, where the attacker can delete, change, coax personal information from one of the parties without both of them knowing.

Spoofing can occur also at higher level protocols as e.g. in SMTP.

For example, **email spoofing** is the forgery of an email header or email addresses where the attacker uses someone else email address in order to send their email so it cannot be traced back to the attacker (Figure 4). Attackers may also use email spoofing so they can impersonate another person or a company to gain access to personal information like bank account etc.

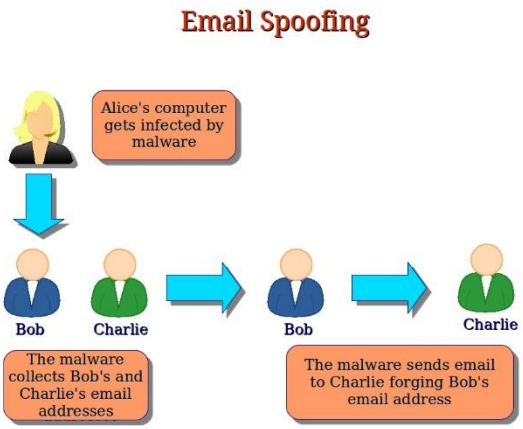

Figure 4 – Email Spoofing

Spoofing can also happen in lower layers of the ISO/OSI stack.

Network level sniffing and spoofing potential threats: 5G NR still lacks the necessary protection to security threats that were evident in LTE networks. Broadcast messages, particularly Master Information Block (MIB) and System Information Block (SIB) packets, contain a myriad of information, not all of which is necessary for the UE to establish a secured connection. Ideally, SIB message content would be limited to strictly what is necessary to establish a radio link with the base station, and further network configuration elements would be shared on a secured and integrity protected broadcast channel. It is necessary to propose methods that allow a UE to determine whether a base station is legitimate prior to executing certain procedures based on the unauthenticated RRC and NAS messages, even though the specifications do not require such mechanism

2.5 Access Attacks

Access attacks allow attacker to gain some form of access to data or machine functionality, which normally, according to the current policy, should not be available. The most powerful form of these attacks is when an attacker gains access to the privileged accounts (for example root on Linux systems or Administrator on Windows systems). Acquiring unprivileged access can be beneficial for the attacker. From the compromised account/machine other attacks can be performed -- for example on machines which are not accessible from public ones. Moreover some exploit can be utilized in order to allow privilege escalation.

Access attacks can be exploited due to incorrect configuration, usage of social engineering or vulnerabilities in the software.

In general, the first two classes of these attacks are associated with the access to the system using login-password pair. Although, this is the simplest and the most popular authentication method, it has many drawbacks. Access to such system can be gained due to:

- easily guessed passwords,
- well-known service or default account/password pairs,
- eavesdropping of passwords due to lack of encryption,
- gaining access to the authorized user’s password due to some form of social engineering.

However, not only knowledge of the password could be used for gaining full access to the computer system. Certain vulnerabilities in the software allow execution of un-trusted, specially crafted code by the attacker. This kind of attack can be exploited if the software contains some types of the code vulnerabilities, commonly called "bugs", for example:

- stack overflow,
- heap overflow,
- format string attacks,
- command injection,
- SQL injection.

Some key points to improve the 5G ACCESS Network are pointed out in 5G security recommendations of the report by_NGMN_5G_Security Group [10 NGMN16]:

- P1: As the network capacity and number of UEs grow, the risk increases that large-scale events could cause significant changes in network traffic patterns, either accidental or malicious. At this scale, it is not possible to differentiate the intent of a network surge and so this recommendation covers both scenarios, although its primary focus is to prevent malicious events.
- S1: The 5G system must wherever possible minimize large swings in traffic usage, and be resilient to them when they do happen, while maintaining an acceptable level of performance.
- P2: User plane data is (in most countries) encrypted, but this provides a limited protection against a Man-In-The-Middle attacker changing that data-en-route, because encryption is linear (a stream cipher) and any checksums are also linear. 3G and 4G include cryptographic integrity protection of (some) signalling messages, but still not for user plane data. Should 5G add integrity protection to user plane data?
- S2: In most cases, the answer is no. The mobile network (visited or home) is not the best place to verify the integrity of user plane data; when data integrity is needed, it will usually make more sense to do this at the transport or application layer, typically terminating beyond the mobile network.
- P3: Overload of the signalling plane by a huge number of infected M2M/IOT devices which simultaneously attempt to gain access to the network
- S3: It is important to study the possibility to modify current overload procedures to be applicable to situations where the overload condition is initiated by malicious actors with sufficient control over the infected devices that they do not comply with network initiated overload procedures.

2.6 Network steganography

Historically, the earliest computer steganographic methods were focused on different media types, especially digital images. As an example, several algorithms were proposed which hide information within the least significant bits of color definitions of pixels within an image as the human eye cannot spot such alterations. Similar approaches have been also utilized for digital representation of audio and video files.

However, during last few years a new trend has emerged where data is hidden in network transmissions, such as in inter-arrival times of packets or in unused fields of protocol headers. Network traffic provides the advantage of a continuous data flow, which a digital

media file of constant size cannot provide. When secret data is hidden in network traffic, the secret communication channel is referred to as a network covert channel.

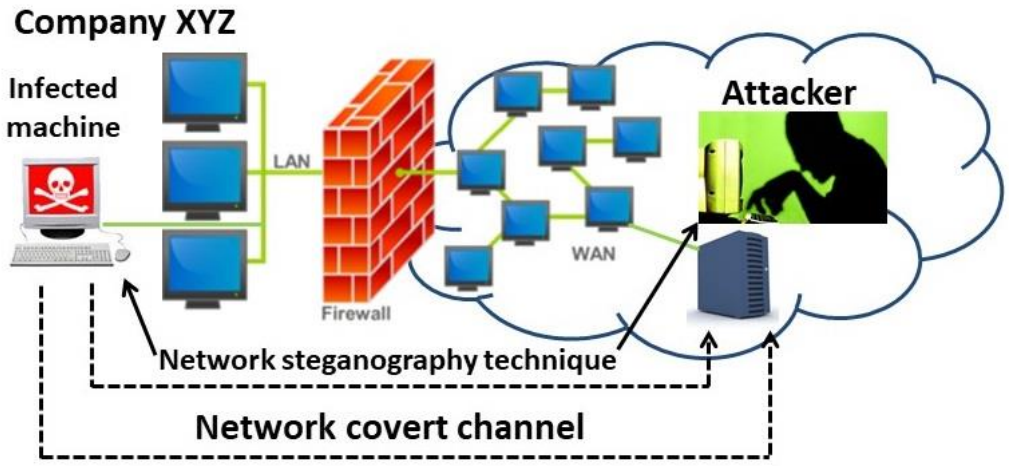

Figure 5 – Hidden communication between infected host and an attacker using network steganography methods

In essence, network covert channels enable secret malware communications over any type of computer network, be it a local area network or the Internet (Fig. 5). Compared to encryption, which only ensures the confidentiality of what a malware communicates, covert channels can help to keep the communication secret, e.g. to retain access to a hacked system. Moreover, control protocols can be used on top of covert channels, representing a form of C&C (Command & Control) channel that are typically used to govern botnets. Such control protocols allow to perform in a stealth manner, for example:

- downloading of a newer version of a malware binary, its component or configuration,
- changing to a different encryption or a covert signing scheme,
- switching from one steganographic method to another,
- exfiltration of confidential e.g. organizational data over the network,
- bypassing firewalls by hiding data in transmissions that are not affected by its filtering policy.

3 Specific IoRL threats analysis

3.1 IoRL short system description

The IoRL system consists of three main components: user equipment (UE), radio access network (RAN) and NFV/SDN part. The developed system will be connected to the outside world using Internet or directly mobile operator using native 4G/5g protocols. The overall architecture is presented in the Figure 6.

During the test scenarios, we will use as UE currently available electronic devices, for example, SMART TV sets, tablets or mobile phones, with a custom device connected by USB used for receiving VLC and receiving and transmitting mmW signal. The RAN part is responsible for providing wireless communication both for VLC and mmW technologies. These functions are provided by so called RRLH (RemoteRadio Light Head) which are built within lights roses. The last element of the IoRL subsystem is responsible for all layer 3 functions. Due to usage of NFV paradigm all new functions of the IoRL system can be added as additional VNFs. Later in this deliverable we present the proposed security monitoring functions implemented as the SDN application.

Such a complex system which uses many technologies introduces some new specific threats. Moreover, each used technology has some weaknesses that could be exploited and poses greater threat for the whole system. In the following paragraphs, the analysis of main used technologies and its threats is presented.

3.2 Security issues in VLC

Several security issues in VLC were discussed in [11]. Although the discussion refers to IEEE802.15.7, it claims to address future VLC techniques as well. For indoor, it considers six different link configurations according to LOS/NLOS and directionality of transmitter and receiver. The author also considers three classes' of VLC devices: infrastructure, fixed and mobile. With respect to these classes basic aspects of security as availability, confidentiality, authenticity and integrity are discussed against threats as: jamming, data modification and eavesdropping (snooping).

VLC PHY Layer Security (PLS): The key point is that the physical channel output is best modelled as a superposition of the outputs of K independent single-user Poisson channels. The general case for K users was analysed by [12] where it was shown that the total throughput is bounded from above. This is in contrast to the Gaussian channel, where total throughput grows unbounded as the log of number of users.

Hence – the multiaccess VLC channel is vulnerable to jamming. A single source (or jammer) with high Tx power will saturate the channel. The same problem can occur by a larger number of rogue low-power transmitters.

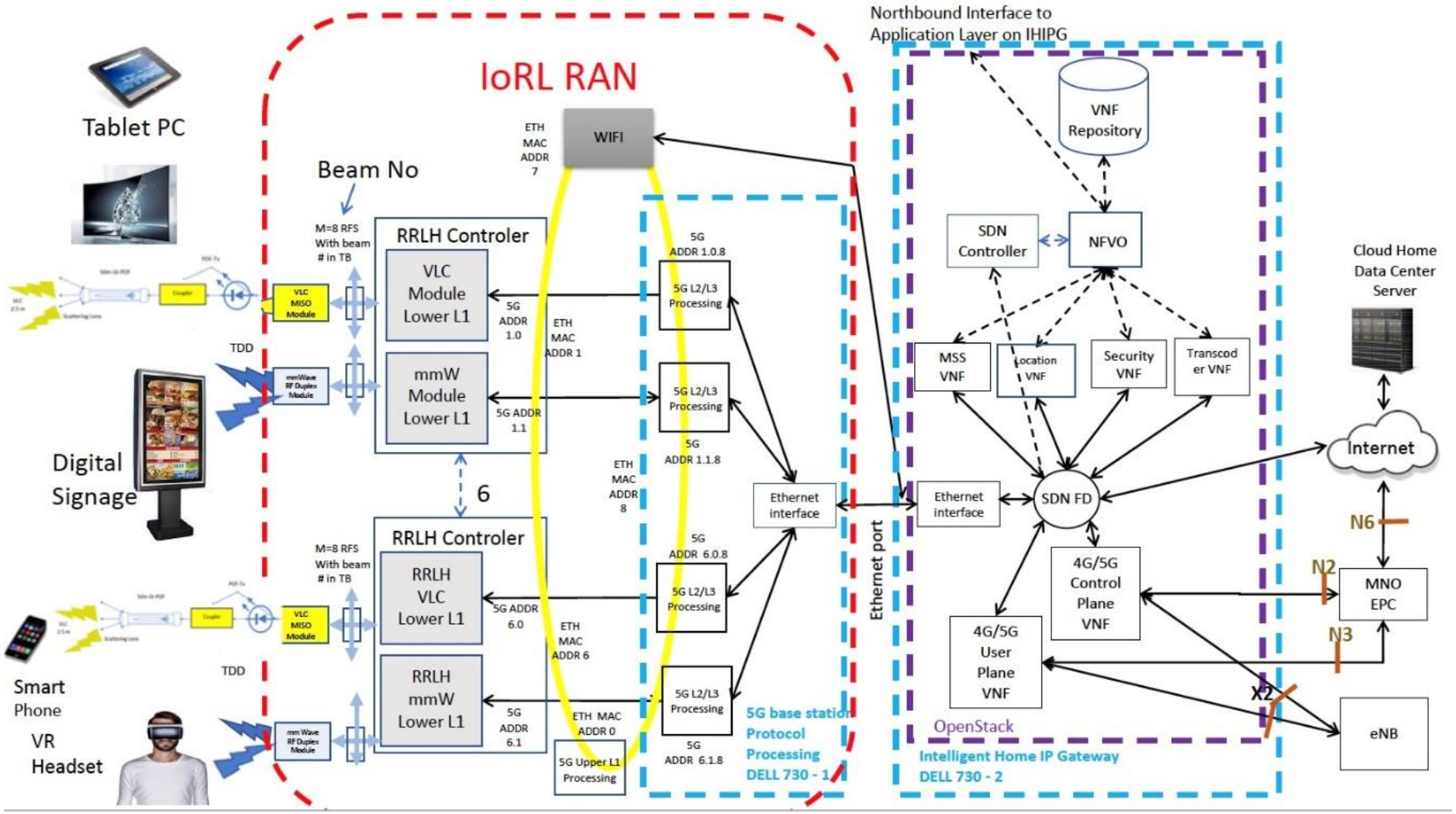

Figure 6 – Architecture of the IoRL system

Other aspects of VLC PLS related to eavesdropping (ED) are discussed in [13]. The case of multiple EDs distributed with Poisson Point Process (PPP) to improve the SNR of EDs over UE is discussed. A closed form metric for secrecy outage probability (SOP) was derived. The bound was derived as a function of the density of EDs and geometric factors related to the indoor VLC environment. The general conclusion is that secrecy performance can be greatly improved by proper selection of transmitter location. [14] has further extended the model to a case where nearest access point (AP) in a multiuser VLC network is assumed. The VLC APs distribution are modelled as two-dimensional PPP, the location of users and EDs are modelled another independent two-dimensional PPP. Results show that cooperating neighbouring APs can enhance the secrecy performance of VLC networks, but up to a limited bound.

VLC security at MAC layer: In IEEE802.15.7 the security mechanism to keep confidentiality and integrity is provided by cryptographical means from higher levels. It is based on symmetric-key cryptography and uses a key shared by higher layers. Cryptographic frame protection is based on link key shared between two peer devices, or a group key among group of devices. Eight security levels are defined:

- **"None"** (no encryption and no integrity)
- **Integrity-only** provided by the Message Integrity Code (MIC) MIC-32, MIC-64, MIC-128
- **Encryption-only**, and
- **Encryption plus MIC** (32, 64 and 128 options)

Encryption in 802.15.7 is based on CCM* algorithm with 128 bits key AES (Advanced Encryption Standard) in the cipher block chaining message authentication code (CBC-MAC).

Table 3-1: Overall wireless security requirements

Security Requirements	**Specific Objectives to be Achieved**
Authenticity	Specified to differentiate users from unauthorised users
Confidentiality	Specified to limit the confidential data access to intended users only
Integrity	Specified to guarantee the accuracy of the transmitted information without any falsification
Availability	Specified to make sure that the authorised users can access wireless network resources anytime and anywhere upon request

3.3 mmW

5G mobile network intends to exploit the available spectrum in millimetre-wave (mmW) band to boost the communication capacity. There are some challenges facing mmW as propagation losses and blockages have to be dealt with.

Table 3-1 shows the overall wireless security requirements and their specific objectives to be able to achieve it. This is believed to be one of the most important things that are needed for the secrecy communication of mmW.

There are two main types of wireless attacks (eavesdropping attack and jamming attack), the physical layer is used for specifying the characteristics of signal transmission, which makes the physical layer extremely vulnerable to attacks. The eavesdropping attack refers to unauthorized user attempting to intercept the data transmission between legitimate users. However, in order to maintain a confidential transmission, cryptography techniques are needed as it relies on secret keys, which prevent eavesdropping attacks from intercepting the data transmission.

3.4 4G/5G

As a starting point for analysis of 4G/5G threat analysis we use document named "5G PPP Phase1 Security Landscape" which was prepared during works of the 5G PPP Security WG. Authors of the document investigate and indicate possible threats to the 5G network.

Prepared list contains eight security risks for 5G:

- Unauthorized access or usage of assets,
- Weak slices isolation and connectivity,
- Traffic embezzlement due to recursive/additive virtualization,
- Insufficient technology level readiness,
- Difficulties to manage vertical SLA and regulation compliance,
- Slicing VS Neutrality,
- Trust management complexity
- Provisions to facilitate change of service provider Domain Lock-in.

Authors of the document after careful analysis of identified threats suggested some basic security requirements that should be introduced into new 5G systems.

The list contains 9 main security requirements:

- Security level,
- Security automation,
- Security monitoring,
- Security management,
- Security liability schemes,
- Inter-tenant/slice isolation,
- 5G liability,
- Enabling value added services with end to end encryption,
- 5G regulation conformity.

What should be pointed out is that from the beginning of the IoRL project the security monitoring (the third requirement) feature was designed to be built-in directly into the IoRL system. More details concerning this functionality of the IoRL system are presented in the section 5.

3.4.1 Security Challenges in Mobile Clouds

In the Network Layer version of the IoRL architecture, the SDN Layer part of the IHIPG can be realized on the building premises, whereas in the Virtual Network Layer version this logical centralized controller can be realized in the Cloud Home Data Center Server (CHDCS) [13]

which can be connected by a tunnel for example using, GRE, IPsec, L2F, L2TP to the RAN. This poses a potential security threat.

Since the resources of cloud computing systems, such as the CHDCS, are realized remotely from the building premises and are shared among users it is possible that a user spreads malicious traffic to tear down the performance of the whole system, to consume more resources or to stealthily access resources of other users. Similarly, in the multi-tenant cloud networks, such as the IHIPG realized on building premises, where MNO tenants run their own control logic, interactions can cause conflicts in network configurations.

The open architecture of Mobile Cloud Computing (MCC) and the versatility of mobile terminals create vulnerabilities through which adversaries could launch threats, which can be classified into front-end, back-end and network based mobile security threats [16].

The front-end is the Smart Phone, Tablet PC, Television and Virtual Reality Headset User Equipment on which applications and interfaces required to access cloud facilities run. Threats to User Equipment largely consist of application level threats such as malware, spyware, and other malignant software employed by rogues to disrupt user applications or gather sensitive user information [17], [18].

The back-end platform consists of the cloud servers, data storage systems, virtual machines, hypervisor and protocols required to offer cloud services where security threats in the form of DoS attacks [19], [20].

Network-based mobile security threats in the form of sniffing, DoS attacks, address impersonation, and session hijacking are targeted towards the Wi-Fi, 4G LTE and 5G Radio Access Networks (RANs) that interface mobile devices to the network. [17], [19]. Distributed Radio Access Network (D-RAN) suffers the threat of single point of failure.

3.4.2 Security Challenges in Communication Channels

The communication in 4G mobile networks can be categorized into three communication channels i.e. data channel, control channel and inter-controller channel. 4G mobile networks have dedicated communication channels based on GTP and IPsec tunnels with communication interfaces, such as X2, S1, S6, S7, which are used only in mobile networks, which are currently protected by using TLS (Transport Layer Security) / SSL (Secure Sockets Layer) sessions [21] and which require significant level of expertise to attack these interfaces.

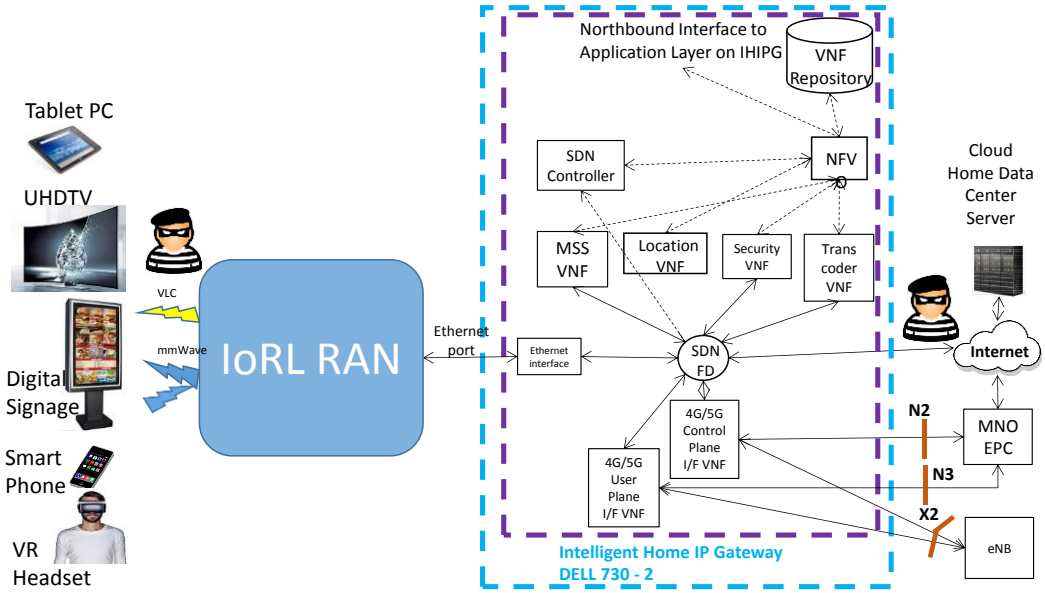

Figure 7 – Mobile Network Operator Building Network

However, TLS/SSL sessions are highly vulnerable to IP layer attacks [19], SDN Scanner attacks [23] and lack strong authentication mechanisms [24].

SDN-based 5G networks may not necessarily have such dedicated interfaces but rather common open SDN interfaces as illustrated in the MNO Building Network architecture in Figure 7 and MVNO Building Network architecture in Figure 8, which will increase the possible vulnerable points for attackers to exploit.

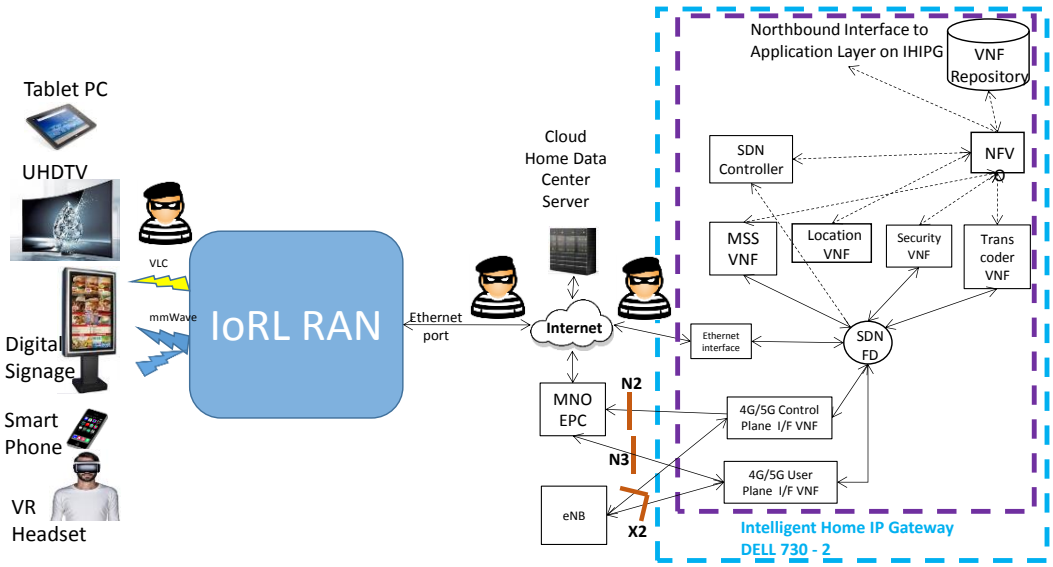

Figure 8 – Mobile Virtual Network Operator Building Network

3.5 SDN

We based our SDN threat analysis mainly on two sources: a paper "SDN A comprehensive study" [25] and ENISA report [2].

In [25] authors perform the threat analysis starting from the SDN network architecture. Figure 9 presents diagram of the sample SDN network, and shows seven points at which network can be vulnerable.

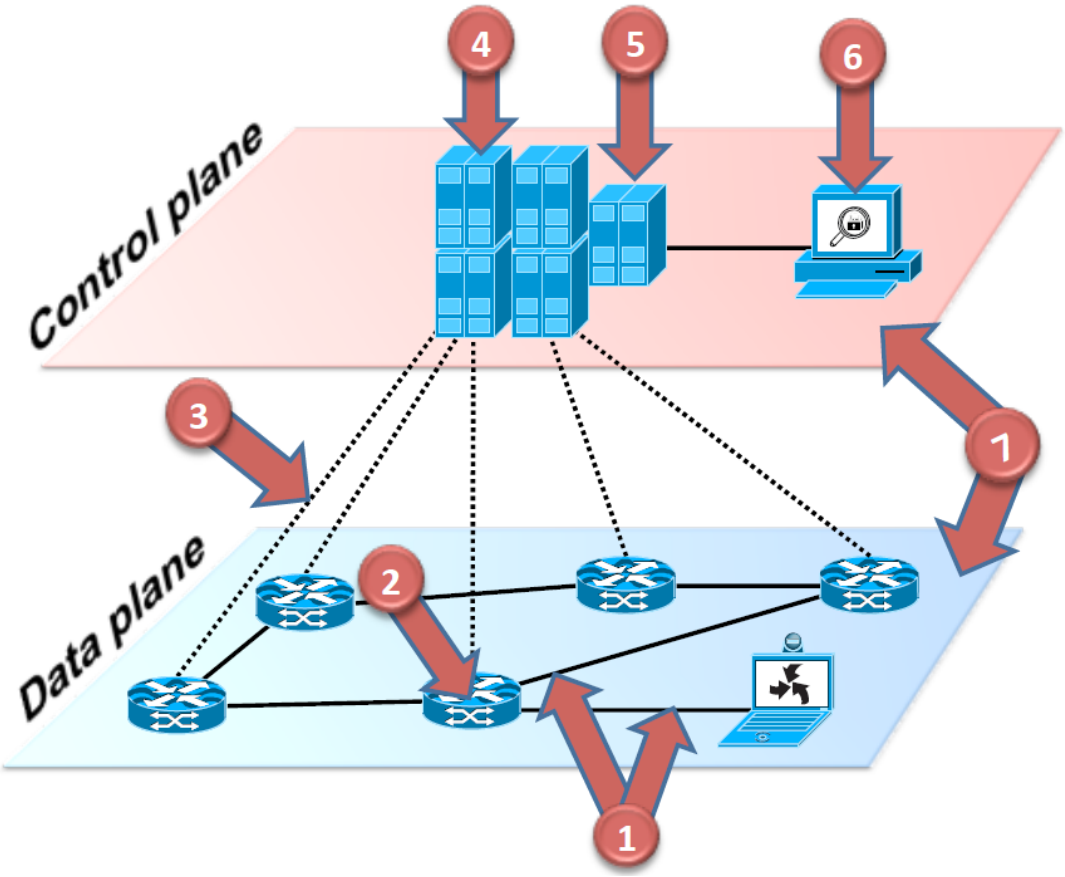

Figure 9 – SDN threats (figure from [25]).

These seven points are:

1. Forgery or modification of the traffic in the data plane.
2. Vulnerabilities in the devices, both software and configuration failure
3. Attacks directed to the control traffic between devices and SDN controller - control plane attacks.
4. Attacks on SDN controller software.
5. Attacks on SDN applications software.
6. Attacks of management stations.
7. Lacks in logging mechanism, especially these for further forensics.

What should be emphasized from these seven points, only three (3, 4 and 5) are specific for the SDN networks. The others, are associated with well-known threats observed in the communication networks and IT ecosystem for years. In most cases they are well-known techniques that can be used for mitigations of these vulnerabilities.

The ENISA report [2] presents the taxonomy of the threats in isolation of the attack place, due to fact that some attacks can be performed in the various locations of the SDN architecture. For example, traffic sniffing can be performed in the compromised SDN switch, using reconfiguration of the SDN network by an infected operator station or using custom

SDN application. However, in this report most of the attacks are directly mapped to ones described in [25].

The ENISA SDN threat model taxonomy identifies the following major threats for SDN networks:

- Data forging,
- Traffic diversion,
- Side channel attack,
- Flooding attack,
- Software/firmware exploits,
- Denial of Service (DoS),
- Identity spoofing,
- API exploitation,
- Memory scraping,
- Remote application exploitation,
- Traffic sniffing.

After careful analysis of all threats presented in the previous paragraphs we introduce some mitigation techniques that should be provided within the IoRL SDN network and supporting IT infrastructure.

Recommendations for the IoRL project:

- Usage of the encrypted and authenticated connections in the control plane - between SDN controller and SDN switches,
- Separation of the user traffic and management/control traffic,
- Addition of the appropriate logging of the policy changes,
- Usage of the SDN applications for detection user specific attacks, for example scanning, DoS etc.
- Hardening of the used SDN devices and virtual servers which execute SDN controller code and SDN applications.

4 Threat analysis of proposed Use Case Scenarios

4.1 Museum scenario

4.1.1 Usage characteristics

The museum is one of the most dangerous scenarios considered in this section, as it is both public with rather open access and a place where users (visitors) spend time in long uninterrupted periods. Because of these characteristics the attacker's job is significantly simplified, as there are many possible target devices and a plenty of time to test their vulnerability.

4.1.2 Phishing, advertisement

If beacons are used to transfer exhibition data when the user is nearby, a malicious device could spoof the presented information and replace it with advertisement or phishing website.

4.1.3 Ticket system

If IoRL technology is used as a way of automatic handling of electronic tickets, the system can be susceptible to mmW beacon jamming, which would prevent the users from entering the exhibition.

4.1.4 Exposure of user devices to hacking attempts

Museum visits usually last a couple of hours, during which the user's device is constantly connected to the museum's network for acquiring the exhibition data. This gives the potential attacker plenty of time to scan the user's device for potential vulnerabilities, exposing him to a potential danger.

4.2 Smart Home scenario

4.2.1 Usage characteristics

Smart Home network environment should be relatively safe in comparison to the networks open to the public, however user devices tend to spend significantly more time attached to the home network than public networks, thus those devices could be exploited in a more stealthy way over long time periods.

4.2.2 Malicious device concealment

Due to the nature of smart home environment, malicious devices can be easily concealed as parts of furniture without raising much suspicion, such as lamp stands or hidden inside objects. Such devices can act as modern Trojan horses - by gifting someone an object containing a rogue device, the attacker could bypass traditional security measures such as a firewall on gateway and attack LAN traffic directly.

4.2.3 Network reconnaissance and DoS attacks

A malicious device placed inside a smart home could connect to the network and perform network reconnaissance by enumerating devices connected to the network and search for

vulnerable services running on those devices. Furthermore, a rogue device could then start a DoS attack on both client devices and network infrastructure, by performing a TCP SYN flood or exhaust DHCP address pool.

4.2.4 Wireless jamming

A malicious device could emit radio or visual waves that interfere with regular wireless communication and jam the network traffic, resulting in a packet loss or DoS attack.

4.2.5 Wireless communication sniffing

VLC communication can be remotely captured with a high speed camera or light sensors by peeking through a window, even if observed over long distances. If VLC transmission was not encrypted, a third party could easily sniff one side of the communication.

4.3 Supermarket scenario

4.3.1 Usage characteristics

Supermarket shares the traits with the Railway Station scenario, as it is a public place, where people tend to spend from 10 to 45 minutes. However, this use case has the disadvantage as people visiting the supermarket are encouraged to download proprietary software on their smartphones to enhance their shopping experience. This poses a social engineering threat, where people can be tricked into installing malicious software on their phones or fall victim to phishing attempts or advertising.

4.3.2 Preparing a shopping list

A customer downloads through a secured link IoRL “Smart Shopping Cart” (SSC) application on his/her smart phone where part of the procedure is providing a credit card account and uses it to prepare a shopping list.

4.3.2.1 Phishing, malware infection

Assuming that each supermarket chain would develop its own application, application executable could be pushed through IoRL channel directly to the user device, posing a threat of malware infection from a rogue access point. For example, a single light bulb placed at the entrance to the supermarket could push a malicious executable that appears to be a legitimate app.

4.3.3 Starting the shopping experience

A customer uses a smart trolley or SSC application to navigate across the supermarket according to the products placed in the list. The SSC calculates the relevant route for the customer and, according to the things written on the list, can offer relevant content (promotions, reviews, recipes and other suggestions). If a product is missing the system can notify the customer and offer relevant alternatives.

4.3.3.1 Code execution

The supermarket will launch an app which will be synchronized with the shopping list on the phone of the user. Depending on the implementation, this could allow attackers to automatically launch any application installed on user's phone or perform arbitrary actions

such as sending an email or SMS message. IoRL enabled devices should implement a proper security system that prompts user whether he wants to execute an action requested by VLC emitter, for example launching an app.

4.3.3.2 Scam, advertising

A fake VLC transmitter hidden on shelf could try to scam the customer, informing him that given product on his list is always unavailable and could promote an alternative product.

4.3.4 Checkout

The SSC is equipped with barcode reader (or similar) which sums up the purchase. When finished with the shopping, the customer just walks out from the supermarket and the system will charge his credit card/ bank account without the need to stop by at the cashier.

4.3.4.1 Scam

Users could install a modified application that would alter the items placed in the shopping cart. For example, it could swap product brands with cheaper alternatives or subtract the amount for purchased products.

4.4 Train station scenario

4.4.1 Usage characteristics

This scenario contains two major use cases, where there are two networks - one is designed for maintenance of the tunnel and is intended only for use by the railway station staff. The second case is a publicly accessible network, where the passengers can browse the Internet, validate their tickets or use the network guide to aid in finding their position.

In case of the maintenance network, the security is crucial for health and safety, thus it should not be publicly accessible. Furthermore, every case of DoS has a huge potential for causing a health hazard, such as by jamming the communication of gas sensors, etc.

In case of the passenger network, this network is publicly accessible and a lot of passengers will pass through it every hour thus as such this scenario has a huge potential for exploitation, especially in case of Man in the Middle attacks.

4.4.2 Accurate location and information provision under train station premises

The Services Manager in the Control Office is able to exactly locate the maintenance workers that are performing activities in the train station or tunnel.

4.4.2.1 Spoofing

An attacker could spoof his location to pretend to be in the middle of the metro tunnel at any given time, possibly causing an alarm and preventing metro trains from departing from the station.

4.4.3 Carbon monoxide and smoke detection in tunnels

This use case installs sensors for detecting carbon monoxide and smoke that can send using IoRL devices, the status information of CO and smoke detectors to the Control Office instantaneously.

4.4.3.1 Health safety

This use case poses a major health safety threat in an event where the communication with the smoke detector is lost or jammed. Unless the device pings its status at regular intervals, in the case of lost connection the device could fail to inform about the danger.

4.4.3.2 Denial of Service

In another scenario, the attacker could register his device in the network as a smoke detector and cause a fake fire alarm that would lead to evacuation. The same applies for altered data from the sensors.

4.4.4 Instant information and ultra-high bandwidth downloading

IoRL devices are used to download information related to services and locations in the street above them (restaurants, how to reach the most appropriate exit for the place where they are heading, what are the most suitable touristic places around, etc.).

4.4.4.1 Phishing, advertisements, malware infection

Depending on implementation, the data containing neighbourhood information could be altered for malicious activities. For example, if the map of the area is presented as an HTML document, this document could be replaced with a phishing website or malware could be pushed to user devices.

4.4.5 Ticket purchase and validation

The security doors to enter the passenger platform will automatically open when holding the cell phone out of the pocket. The IoRL technology will automatically detect those cell phones that are providing the information related to the ticket. No action from the passenger will be needed, only holding the cell phone in the hand. People need to buy a ticket on their mobile in order to pass through VLC barrier.

4.4.5.1 Denial of Service

mmW communication could be jammed at the entrance, preventing user devices from transmitting their ticket data and preventing security doors from opening.

4.4.5.2 Scam

Tickets encoded on user devices could be altered with specialized software (for example: an Android application could prolong ticket's expiration date).

4.4.6 Commercial signage

The digital sign could point out and show directions and routing info as well as more neighbourhood related information such as exit routes from the station and local business offerings in and outside the station.

4.4.6.1 Phishing, advertisements

Multimedia streams could be modified to include advertisements or encourage users to type in personal data.

4.5 Conference scenario

4.5.1 Usage characteristics

This is similar to the museum scenario because the users attending the conference usually have something in common, thus the attack can be more targeted and have a higher chance of success.

4.5.2 Exposure of user devices to hacking attempts

The conference usually lasts a couple of hours, during which the user's device is connected to the provided network. This gives the potential attacker a plenty of time to scan the user's device for potential vulnerabilities, exposing him to a potential danger.

4.5.3 Phishing, scam

Some form of conference information (schedule, building schema etc.) could be provided via a local website which requires creating an account. A potential attacker could set up a fake site and collect passwords. Because not every user uses unique passwords for every service, such database could be used to hack other accounts such as e-mail, bank or social media.

5 Integrated Security Framework

5.1 ISF overview and main components

The main aim of the ISF (Integrated Security Framework) is related to the detection of various attack types directed to or sourced from IoRL RAN, for example, Denial of Service attacks, or hostile scanning activity. The ISF will be deployed at the IHIPG-2 as a NFV. The main parts of the ISF are:

- Virtual Machine containing main detection programs,
- SDN security monitoring and management application,
- Web-based security Dashboard.

Figure 10 presents the ISF elements deployment in the IHIPG-2 system.

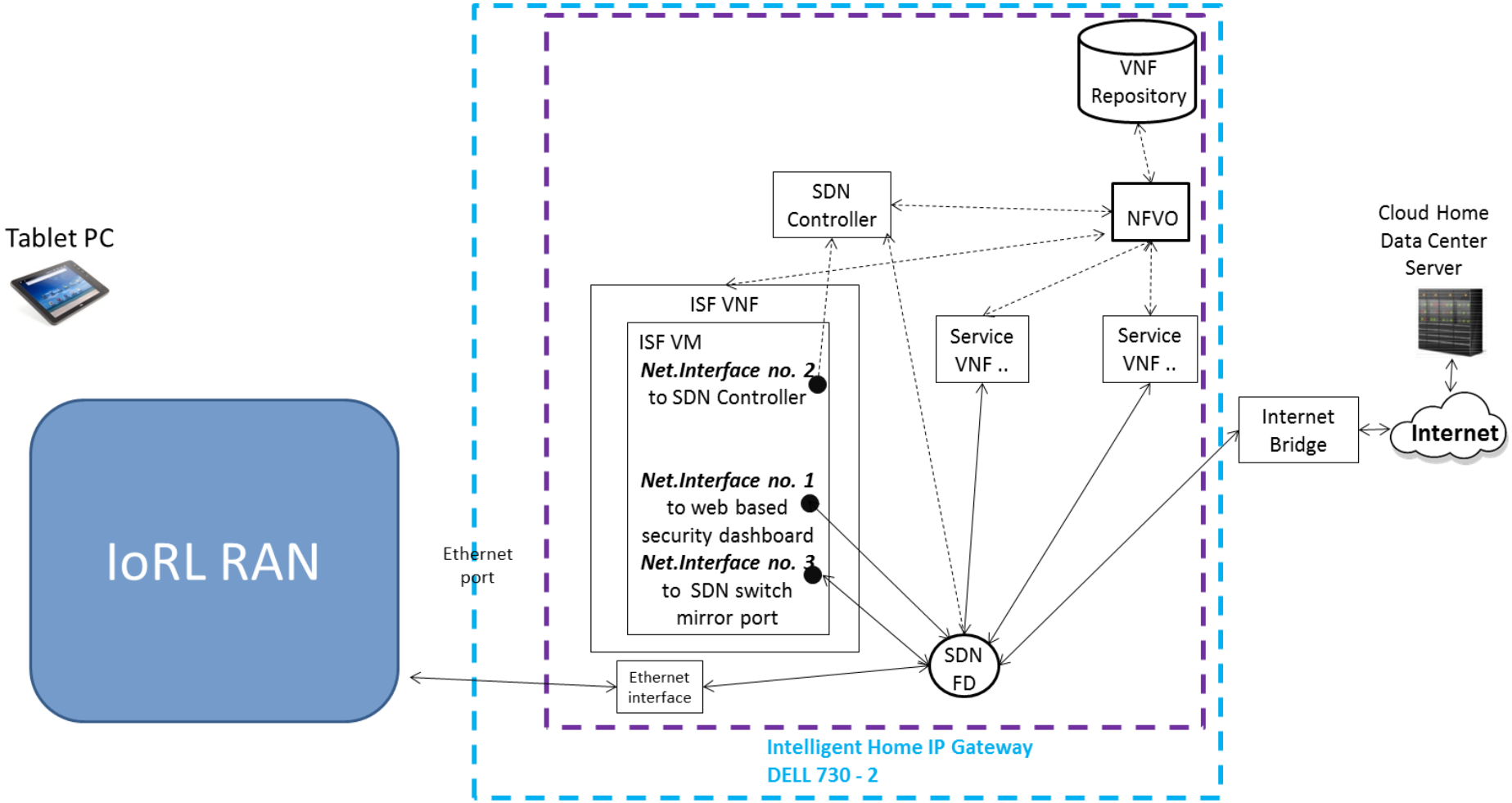

Figure 10 – ISF in IoRL IHIPG-2

In the remaining of this document we will describe the three main ISF components mentioned above.

5.2 Virtual Machine

Virtual machine deployed by the NVF orchestrator is the main part of the ISF subsystem and hosts all security-related programs developed during the project. Virtual machine contains three network interfaces that connect it to the IoRL internal SDN network. The first interface is accessible from the users connected to the IoRL RAN. This interface is used for accessing security dashboard (described in detail later) which allows administrators' access to the ISF configuration and viewing logs generated by the ISF. The second interface is used as management interface, which allows communication between ISF monitoring application and the SDN controller. The last, third interface is used as a SPAN/mirror port in order to direct interesting or suspicious IoRL RAN traffic for further security-related analysis. The traffic directed to this port is dynamically configured by the security application using management interface.

The deployed virtual machine is controlled by Linux operating system and hosts various programs which in cooperation implements all ISF functions. In the following sections, the most import parts of the system are described with details.

5.3 SDN security monitoring and management application description

The main logic of the ISF is developed as an SDN application. The application interacts with the SDN controller in two ways. First, it uses SDN controller as a source of data for further analysis. Due to performance reasons network traffic analysis is not performed directly at the SDN controller. Instead a copy of interesting or suspicious traffic will be forwarded to the dedicated application executed at the ISF virtual machine. Secondly, when some hostile activity is detected, mitigation actions which reconfigure SDN network are performed, for example, dropping/blocking hostile traffic.

There are two possibilities to implement SDN application. The first one needs integration of the SDN application code directly into SDN controller. The second one utilizes standalone application, which uses one of defined northbound interface API. Currently, the final decision regarding this aspect has not been reached as this requires further arrangements with NCSRD partner responsible for SDN/NVF part of the IoRL system.

Apart from the SDN application which directly interacts with the SDN network in the ISF virtual machine dedicated Linux daemon is executed, later in this report called analysis Security Analysis & Mitigation Service (SAMS) daemon/service/application/program. This service is responsible for the analysis of interesting or suspicious copy of the network traffic, which will be forwarded accordingly to the custom flow rules prepared by the SDN application. SAMS listens to all raw traffic on the dedicated (third) interface of the ISF virtual machine. Acquired packets are parsed and later analysed. In case that attack or other anomaly is detected the appropriate information is logged for the user/administrator for further investigations. Additionally, if the detected behaviour is identified as evident attack according to the user/administrator configuration an automatic attack mitigation procedure can be implemented. For this purpose SAMS exchanges information with the SDN application and custom flow rules are installed in the SDN switch.

5.4 Security Dashboard

The chosen users of the IoRL system (e.g. administrators) depending on the place of installation, for example, home, supermarket or train station are allowed to reconfigure ISF and/or view logs and alerts generated by the ISF system. Later in the document such users are defined as IoRL ISF administrators. All these actions are performed using web-based security dashboard, which is the main way of accessing security-related functions of the system.

As mentioned the security dashboard is implemented as a web application hosted on the standard web server. Currently there is no firm decision, however Apache or Nginx as a web server and PHP or Python with Django framework are considered as elements used during ISF implementation. The web interface of the security dashboard is accessible from the UE connected to the IoRL RAN using Sec_IP. Sec_IP is dedicated IP address configured during IoRL system deployment only for security dashboard purposes.

5.5 Integration of location services for network security purposes

Location estimation services are performed using VLC and mmW parts of the IoRL system.

In the mmW location service, the last 14th OFDM symbol (as shown in Figure 11) of the 1st 2nd 3rd and 4th sub-frames of a 5G Transport Block (as shown in Figure 12) are used for the user equipment to transmit the Sounding Reference Signal (SRS) with predefined Zadoff-Chu Sequences of no fewer than 48 predefined sub-carriers locations on 14th OFDM symbol and the RRLH receiver records the delay SRSs from different UEs on the last 14th OFDM symbols of the 1st 2nd 3rd 4th sub-frames. In a 100 MHz Channel Bandwidth and SCS = 60µs, there are 132 Resource Blocks or 12*132 = 1584 subcarriers so for a minimum of 48 Subcarriers per SRS this will allow SCSs from up to 33 UEs to be transmitted simultaneously – more than enough for the IoRL project. So in the IoRL project the allocations of the Zadoff-Chu Sequences of no fewer than 48 predefined sub-carriers locations on 14th OFDM symbol will be predefined. This means that a measurement is obtained every 2.5ms, which when averaged over 8 measurements and sent the result back to the location database every 20ms within the RLC / PDCP protocols, which will arrive at the SDN FD as a PDCP packet which will be forwarded to the Location Database for processing. That makes it 50 mmW location measurements per second. Averaging over 16 measurements will reduce the number of measurements reported to the Location Database to 25 mmW location measurements per second. In a commercial system there will more than likely be more than 33 UE in a RRLH Coverage area and so a scheduling scheme, most probably administered by the Location Server on the IHIPG, will be required to schedule groups of 33 UE at a time in its location area to report their locations.

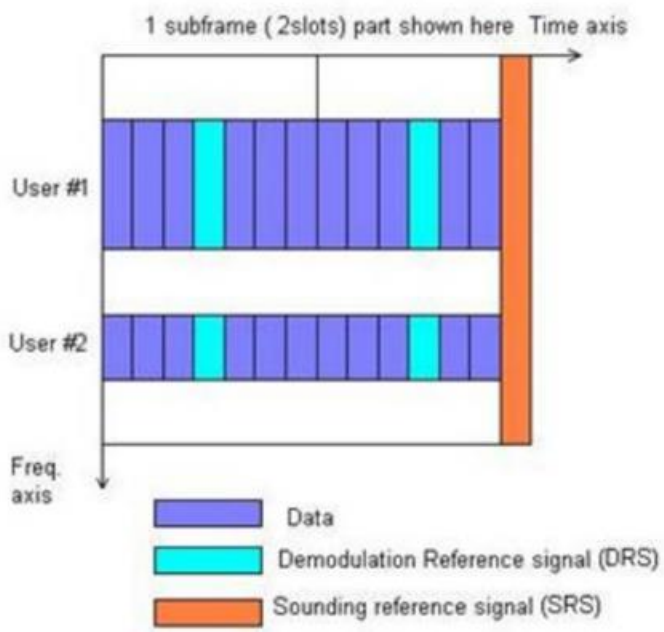

Figure 11 – Location of a Sounding Reference Signal (SRS) in an Sub-frame.

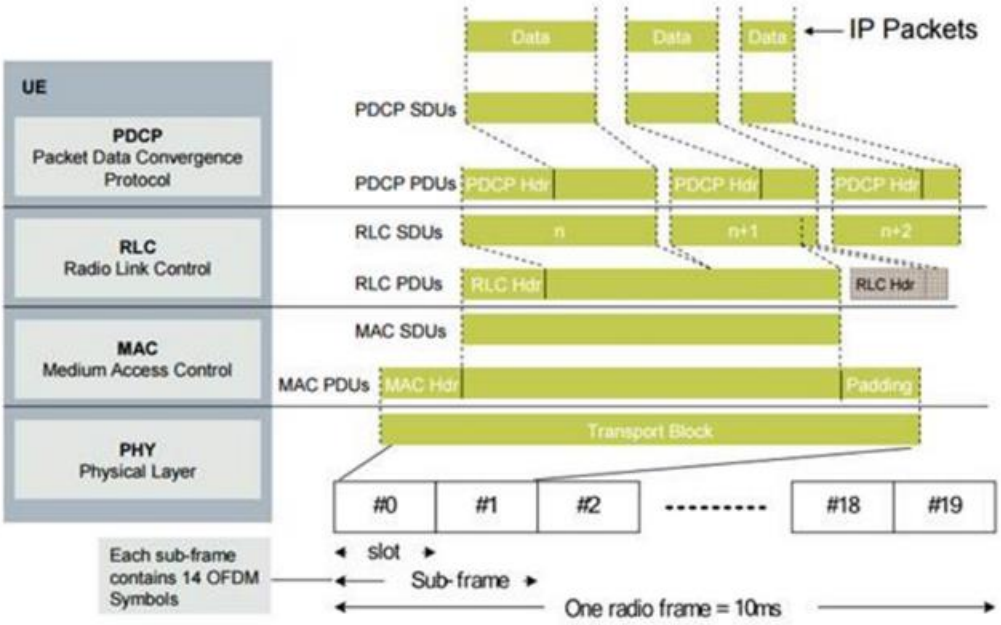

Figure 12 – Transport Block Structure

In the VLC location service, the last 14th OFDM symbol of the 1st 2nd 3rd and 4th sub-frames of a 5G Transport Block (as shown in Figure 12) are used to transmit a OFDM to only one of four RRLH VLC transmitters in turn so that UE knows which RRLH is transmitting and use the RSS information to estimate distance from it. This means that a measurement is obtained every 2.5ms, which, when averaged over 8 measurements, is sent the result back to the location database every 20ms using IP Packets.

6 Integrated Security Framework Demonstration of the Selected Scenarios

6.1 (D)DoS attacks, detection and mitigation

6.1.1 DHCP exhaustion

The attacking host introduces itself multiple times as a new host in the network (using random MAC addresses in DHCP packets) and requests IP address from the DHCP server.

The pool of available addresses has limited size thus when exhausted, no new clients are able to obtain new IP addresses. In such a situation new DHCP Discover messages will be ignored by server resulting in a successful DoS attack where no new real host can receive an IP address and connect to the network.

Due to the design of DHCP system, the DHCP server has no possibility to determine whether a DHCP request is legitimate or not. In order to detect the malicious DHCP requests, a more complicated approach is required.

We are developing a POX SDN module, which keeps track of DHCP queries and monitors the behaviour of machine requesting the address.

The first DHCP REQUEST sent by the given MAC address is always dropped for basic protection against the most common DHCP exhaustion attack, as simple bots only send one DHCP REQUEST packet per MAC. This does not interfere with most clients, as they continue to send DHCP REQUESTS until they receive a DHCP OFFER by using a retransmission strategy that incorporates a randomized exponential back-off algorithm.

However, a more sophisticated method is required to detect more cunning attackers. We attempt to detect spoofed DHCP requests by implementing an algorithm in our module that keeps track of timing between DHCP packets and determines whether the timing matches a set of predefined patterns of most common client devices - Microsoft Windows machines and Android smartphones. By tracking the time between each DHCP retransmission and comparing them to the predefined pattern, we can accurately distinguish between real DHCP clients and spoofed requests generated by malicious software.

6.1.1.1 Scenario

The attacker connects to the network and launches a shell script that repeatedly forges DHCP REQUEST packets with random MAC address.

A benign user tries to connect to the network shortly afterwards.

6.1.1.2 Without DHCP exhaustion module

The attacker quickly obtains all available addresses in the DHCP address pool and effectively starves the DHCP server’s address pool. The benign client will not get an IP address assignment and has been denied the service.

6.1.1.3 With DHCP exhaustion module

If the attacker used a simple script that sends a single DHCP REQUEST, he would not receive a single IP address from the server, as the first packet in a transaction is always dropped by the SDN controller.

If the attacker used a more sophisticated method, but still used an artificial shell script to forge DHCP requests, then he would still be unable to starve the DHCP address pool. However, in case of the attacker that mimics the DHCP traffic perfectly, we should resort to using a dedicated method for detection of malicious clients in the network.

Currently one of the fairly frequent cases of network attack involves spoofing of packets/frames source address, where attacker conceals his identity in the network in order to either attack other hosts or the network infrastructure itself. In LAN, a learning network switch in order to perform its function, must keep track which device (identified by its MAC address) is connected to a physical interface port. This information is usually kept in memory in a forwarding/switching table of a fixed size and updated whenever a frame with new MAC address is encountered. Because MAC address can be spoofed, it is possible to fill the forwarding table completely by intentionally sending bogus frames to the switch. This in turn forces the switch to broadcast all frames to all ports (except the one on which they were received) which as a result effectively transforms switches into a simple network hub. In such a case the attacker is able to sniff all network traffic that is reaching this intermediate device.

6.1.2 MAC Spoofing

We are developing a POX SDN Controller module which limits the number of devices (their MAC addresses) that are allowed to send packets to a particular interface on the switch by keeping a list of “known” MAC's. Packets sent from unknown hosts when the list is full are silently dropped. Total number of allowed MAC's per interface should sum up to maximum capacity of the switch routing table. This way switch will never enter broadcast mode, making it impossible to sniff passing traffic.

6.1.2.1 Scenario

The attacker connected to the network tries to fill the MAC table entirely by running dsniff’s utility “macof”. This utility generates packets with spoofed source MAC address and quickly fills the learning switch’s MAC table.

6.1.2.2 Without MAC spoofing detection module

Switches without Port Security quickly overflow the MAC table and start to broadcast the packets to all ports instead of forwarding them to selected ports. This way the attacker has the possibility to sniff on traffic passing through the network.

Switches with Port Security will automatically disable the entire network port.

6.1.2.3 With MAC spoofing detection module

When the MAC table is close to overflow, the learning switch will stop to accept new packets originating from MAC addresses not already present in the MAC table. At the same time, the traffic originating from already known address remains unaffected.

Additionally, the MAC detection module should raise a warning to the system to trace the location of malicious device.

6.2 Scanning activities detection and mitigation

The aim of scanning activity is to find potentially vulnerable machines and enumerate all the services running on them. In most cases this process precedes actual attacks. Due to this, early detection of scanning activities is beneficial and gives valuable time to prepare network for further attacks. Moreover, if the security system introduced in the network can early detect and prevent network from full scanning activity further attacks can be limited.

Currently there are many different types of scanning, however, the most popular is TCP SYN scan. In summary, an attacker is attempting to determine the state of every TCP port of the target IP address (65536 ports in total) without establishing a full connection. This is achieved by sending a SYN segment addressed to every port on the server. If the server responds with SYN/ACK, it means the port is open. If the server responds with an RST segment then this indicates that the port is closed but reachable. If there is no response after a specified amount of time, then typically it means that the packet has been filtered out by the firewall and the target port is unreachable.

We are developing and evaluating a TCP SYN scan detection and mitigation module for POX SDN Controller. The module works by tracking the state of each TCP connection in the traffic handled by the switch.

When a client attempts to initiate a TCP connection (a SYN packet is sent), the controller creates a description object (IPv4 addresses, ports) and sets its state to pending. This state will not change until a full TCP handshake is completed, in which case the status of this connection changes to connected. When the connection is closed (either via RST or FIN flag) the description object is removed.

By counting the number of pending connections per client IP address we are able to distinguish a scanning machine from a benign one. Because even legitimate TCP connections sometimes fail, we focus not on a raw number of pending connections, but on the rate of their appearance - we count the connection attempts occurring within a predefined time window. If this number exceeds a certain value (i.e. threshold), that particular host (client IP address) is probably trying to scan the network - the controller instructs the switch to drop packets from this IP address for a configurable amount of time (i.e. ban time).

We have assessed the performance of our module and optimized the algorithm in order to prevent unintended DoS on the SDN controller. We have separated the algorithm into two separate parts - the first one is executed every time a new packet is received by the controller and is solely responsible for keeping the track of the connection. The second part runs periodically (by default once per second) and executes CPU heavy operation of counting the per IP summary of TCP connections to ban the hosts that exceed given threshold value.

6.2.1 Scenario

The attacker host “iorl_01” tries to enumerate every TCP service running on host “iorl_nas”. The host “iorl_nas” is a Network Attached Storage that has active SSH, FTP, HTTP and SMB services.

The attacker runs nmap tool to determine the state of all 65536 TCP ports. Nmap tool probes the TCP ports in random order.

6.2.2 Without TCP SYN detection module

After few minutes of running nmap tool, the attacker has enumerated all services running on the “iorl_nas” host and has the possibility to detect their version and exploit potential vulnerabilities.

6.2.3 With TCP SYN detection module

The first few TCP SYN packets sent by “iorl_01” host pass through the network switch uninterrupted. However, when the number of unfinished connections exceeds a given threshold, all packets sent by the “iorl_01” host are dropped.

Because the nmap tool probes the ports in random order and the “iorl_nat” has a relatively low number of open ports, it is unlikely that the attacker will find any open service while sending the initial few packets.

6.3 Rogue device placement

Every wireless and publicly accessible network is vulnerable to rogue clients that attempt to connect to the network and perform malicious actions, such as network eavesdropping, man in the middle attacks or exploiting the services and devices running the network. In case of IoRL and multipath wireless communication this vulnerability poses a severe security threat. For example, a malicious third party could set up a fake access point that acts as a man in the middle proxy.

6.3.1 Handover with malicious access point

The IoRL solution offers the possibility for user equipment devices to seamlessly roam across the coverage area of multiple access points, including traditional WLAN, LTE, mmW and VLC. The handover between multiple access points is done automatically based on a number of variables and metrics.

The decision which Radio Access Network (RAN) to choose is made by user terminal using one of multiple strategies evaluating the following qualities: Network metrics, Device-related metrics, Application requirements and User Preferences.

In particular, network metrics include information about the technical characteristics or performance of the access networks, such as: technology type, coverage, security, pricing scheme, monetary cost, available bandwidth, network load, latency, received signal strength, blocking probability, network connection time, etc.

Those metrics due to their abstract nature are defined by network administrator instead of being measured, thus are advertised by access point to all the clients as-is. A malicious access point could fake those values and advertise itself as the best possible connection, effectively allowing him to route the traffic from all available devices in its range. This exposes the connected devices to fall victim to traffic monitoring or Man in the Middle attacks, such as DNS hijack. This scenario could be exploited in use cases including public places, such as a railway station.

The main feature to the attacker is to effectively pose as a legitimate access point in IoRL network. The attacker has to connect as a regular user to IoRL network and then create an access point. Due to wide adaptation of modern smartphones capable of creating a 802.11n/ac hotspot, this attack would not require specialized hardware.

One possible mitigation of this attack is to require all access points to provide a valid public certificate that matches the IoRL network.

6.3.2 Access point identity verification

At the moment, IoRL does not specify a method for client devices to verify the identity of IoRL infrastructure's endpoint devices, such as WLAN Access Points or VLC emitters. The attacker needs only basic information about the network to perform an attack - in order to spoof a WLAN access point it only needs BSSID and optional network password, which probably is already known to public. This poses a security threat, as the client device has to blindly accept any access point, assuming that it is safe and belongs to the intended IoRL network. Moreover, currently there is no specified handshake protocol to initiate a session between client device and IoRL network. Obviously IoRL includes many well-defined communication protocols that provide session management on their own, such as 802.11ac or 802.11ad, but in the IoRL's case we believe that the client should be informed up front about all the metadata necessary to establish a secure connection, such as:

Root certificate - all network endpoints should announce to user their public certificate signed by the root certificate.

List of available technologies - informs client about communication channels available in the IoRL network - mmW, LTE, WLAN, VLC.

List of available access points - contains description of AP, such as BSSID, MAC address, their capabilities and quality of service.

Shared password to WLAN/mmW networks - WLAN networks without password suffer from lack of encryption. Providing even a basic password secures the communication between client and AP.

Using public certificates in proposed handshake provides a method for client device to verify the identity of surrounding access points, however every certificate chain needs a proper trust anchor. This solution is not perfect, because an attacker could issue his own self-signed root certificate and announce it to the client.

6.3.3 Active monitoring of malicious access points

The method proposed in Access point identity verification could be used as a countermeasure against malicious access points. Every endpoint device connected to IoRL infrastructure could actively scan for all available devices and identify those that attempt to spoof a legitimate device. In case of detection of a rogue device, the SDN controller could be instantly informed about the threat to prevent escalation of attack (for example by isolating traffic to the device). Moreover, the proposed triangulation process could be used to locate the physical location of the rogue device.

6.3.4 Injection of virtual network equipment into SDN Architecture

Many use cases covered in IoRL project deal with networks targeted towards public audience, such as museum visitors or railroad station users. In those cases a rogue user could potentially disrupt the network architecture by registering with SDN Controller as a fake network device such as a network switch or an access point.

At this moment, OpenFlow lacks an implementation for proper Transport Layer Security communication and certificate exchange, thus any device could connect to the network and advertise itself as a router. However, IoRL project has declared to address this issue by implementing an API for providing a secure certificate exchange.

7 Summary

In this deliverable an in-depth analysis of each components of the IoRL system has been performed. The main threats have been identified and an Integrated Security Framework have been designed and developed in order to counter them. Moreover, each assumed IoRL use cases have been investigated from the security perspective. Finally, some exemplary scenarios to demonstrate how ISF can be efficiently used to counter selected threats have been presented.

References

[1] 5G PPP Security Work Group, 5G PPP Phase 1 Security Landscape, June 2017, URL: http://5gensure.eu/files/5g-pppwhite-paperphase-1-security-landscapejune-2017pdf

[2] ENISA, Threat Landscape and Good Practice Guide for Software Defined Networks/5G, December 2015, URL: https://www.enisa.europa.eu/publications/sdn-threat-landscape/at_download/fullReport

[3] CHARISMA, Deliverable D3.2: Initial 5G multi-provider v-security realization: Orchestration and Management, August 2015, URL http://www.charisma5g.eu/wp-content/uploads/2015/08/CHARISMA-D3.2_v1.0.pdf

[4] SELFNET, Deliverable D2.1: Use Cases Definition and Requirements of the Systems and its components, October 2015, URL: https://bscw.selfnet-5g.eu/pub/bscw.cgi/d18783/SELFNET%20Deliverable%202.1%20-%20Final%20v12.pdf

[5] VirtuWind, Deliverable D3.2: Detailed Intra-Domain SDN & NFV Architecture, January 2017, URL: http://www.virtuwind.eu/_docs/deliverables/VirtuWind%20Deliverable%20D3.2%20%20Detailed%20Intra-Domain%20SDN%20&%20NFV%20architecture.pdf

[6] MALTSEV, A., MASLENNIKOV, R., SEVASTYANOV, A., KHORYAEV, A., LOMAYEV, A. Experimental investigations of 60 GHz wireless systems in office environment. IEEE J. Selected Areas in Communications, 2009, vol. 27, no. 8, p.1488-1499

[7] Ignacio Marin-Garcia et. Al, "Study and Validation of Eavesdropping Scenarios over a Visible Light Communication Channel," Sensors 2017, 17, 2687

[8] Classen, J., Chen, J.; Steinmetzer, D., Hollick, M. and Knightly, E. "The Spy Next Door: Eavesdropping on High Throughput Visible Light Communications,". In Proceedings of the 2Nd InternationalWorkshop on Visible Light Communications Systems, Paris, France, 11 September 2015; ACM: New York, NY, USA; pp. 9–14.

[9] Lichtman et al. "5G NR Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation, "IEEE International Conference on Communications (ICC) Workshops - 1st Workshop on 5G Wireless Security (5G-Security), pp. 1–6, May 2018.

[10] NGMN 5G security group, "5G security recommendations Package #1," 6th May 2016

[11] G. Blinowski , "Security issues in visible light communication systems," IFAC-PaperOnline 48-4, pp. 234-239, 2015

[12] A. Lapidoth and S. Shamai, " The Poisson multiple-access channel," IEEE Trans. on Information Theory, 44(2), pp.488-501, 1988.

[13] Cho. et al. "Physical layer security in visible light communication systems with randomly located colluding eavesdroppers," DOI 10.1109/LWC.2018.2820709, IEEE Wireless Communications Letters (early publication),

[14] L. Yin and H. Haas, "Physical-layer security in multiuser visible light communication network," IEEE J. on Sel. Areas Commun. Vol. 36 no.1 pp. 162-174, Jan2018

[15] Yue Zhang, John Cosmas (editors) "System Functional Requirements and Architecture" IoRL Deliverable D2.2, 1st February 2018

[16] Ijaz Ahmad, , Tanesh Kumar, , Madhusanka Liyanage, , Jude Okwuibe, , Mika Ylianttila, , Andrei Gurtov "5G Security: Analysis of Threats and Solutions" 2017 IEEE Conference on Standards for Communications and Networking (CSCN)

[17] S. S. Vikas, K. Pawan, A. K. Gurudatt, and G. Shyam, “Mobile cloud computing: Security threats,” in 2014 International Conference on Electronics and Communication Systems (ICECS), Feb 2014, pp. 1–4.

[18] M. L. Polla, F. Martinelli, and D. Sgandurra, “A Survey on Security for Mobile Devices,” IEEE Communications Surveys Tutorials, vol. 15, no. 1, pp. 446–471, First 2013.

[19] H. Suo, Z. Liu, J. Wan, and K. Zhou, “Security and privacy in mobile cloud computing,” in 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC), July 2013, pp. 655–659.

[20] A. Chonka and J. Abawajy, “Detecting and Mitigating HX-DoS Attacks against Cloud Web Services,” in 2012 15th International Conference on Network-Based Information Systems, Sept 2012, pp. 429–434.

[21] M. Liyanage, A. B. Abro, M. Ylianttila, and A. Gurtov, “Opportunities and Challenges of Software-Defined Mobile Networks in Network Security,” IEEE Security Privacy, vol. 14, no. 4, pp. 34–44, July 2016.

[22] M. Liyanage, M. Ylianttila, and A. Gurtov, “Securing the control channel of software-defined mobile networks,” in Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, June 2014, pp. 1–6.

[23] S. Shin and G. Gu, “Attacking software-defined networks: A first feasibility study,” in Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, ser. HotSDN ’13. New York, NY, USA: ACM, 2013, pp. 165–166. [Online]. Available: http://doi.acm.org/10.1145/2491185.2491220

[24] M. Liyanage, A. Braeken, A. D. Jurcut, M. Ylianttila, and A. Gurtov, “Secure communication channel architecture for Software Defined Mobile Networks,” Computer Networks, vol. 114, pp. 32 – 50, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128617300075

[25] D. Kreutz, F. V. Ramos, P. Verissimo, C. Rothenberg, S. Azodolmolky, S. Uhlig. “Software-Defined Networking: A Comprehensive Survey”, Proc. of the IEEE, 103(1):14-76, January 2015

