Cyber-threats: what is it?

The exposure of an assets to threats
What are the parts?

• Assets
• Vulnerabilities
• Controls
• Threats
• Threat Agents
• Attack methods (vectors)

...and interconnections thereof is Threat Intelligence!
What is ENISA Threat Landscape

<table>
<thead>
<tr>
<th>Collect</th>
<th>Collate</th>
<th>Analyse</th>
<th>Set Context</th>
<th>Disseminate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor 1 Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor 2 Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor n Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agency Study</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R&amp;D NGO Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CERT Advisories</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feed Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ENISA Threat Analysis Process

- Collect
- Collate
- Analyse
- Set Context
- Disseminate

ENISA Processing

- Identify Top Threat Types
- Threat Types
- Threat Agents
- Sectorial Threat Landscape
- Protective Controls
- Asset Types
- Information Dissemination

Structure Data
From Threat Info to Intel...

ENISA Threat Landscape

- Threat Information Collection
- Threat Information Collation
- Threat Analysis
- Set Threat Context
- Information Dissemination

ENISA Thematic TL

Find reliable sources

Isolate and relate similar information

Evaluate findings and decide what to take on board

Find out practices, issues, vulnerabilities, risks, etc.
Why this work on 5G/SDN

• 5G represents the next major phase of mobile telecommunication systems and network, aiming at extreme broadband and ultra-robust, low latency connectivity

• Strong interconnection and key enabler for the development of future technologies (IoT, Smart cities, Intelligent transportation...)

• 5G will be driven by the influence of Software Defined Networking (SDN) and Network Function Virtualization (NFV).

• The key concept that underpins SDN is the logical centralization of network control functions by decoupling the control and packet forwarding functionality of the network.

• Needed to provide a comprehensive account of the emerging threat SDN/5G landscape:
  • By identifying related network assets and the security threats, challenges and risks arising for these assets.
  • Review and identify existing security mechanisms and good practices for SDN/5G/NFV.
What 5G network architecture will bring

- Integrate multiple radio access technologies in licensed and unlicensed frequency bands.
- Mobile edge computing will bring the cloud i.e. applications, content and context closer to user locations. This will personalize the service experience through faster service delivery.
- Virtualization of core and radio access network functions will optimize the use of network resources, add scalability and agility.
- SDN technologies will enable transport network resources, including fronthaul and backhaul, to become virtually programmable.
- A shared data layer will emerge to provide a single version of all network data.
- Big data analytics will support cross-layer orchestration and enable real-time action to be taken.
- Networks will become self-aware, cognitive, and implement extensive automation and continuous and predictive learning.
- Security and end-to-end management and orchestration will be embedded into the network architecture across all domains, operators will gain a programmable network architecture.
5G/SDN Architecture

Figure 2 - Typical SDN Architecture Topology

Figure 3 - 5G architecture
## SDN Architecture and 5G design principles

<table>
<thead>
<tr>
<th>SDN Architecture</th>
<th>5G design principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>The Data Plane</strong> is responsible for the data forwarding functionality of the network and realized through a set of physical network devices (network elements).</td>
<td>• <strong>The infrastructure resource layer</strong> contains any physical device including mobile devices, Internet of Things (IoT) devices etc. (5G devices), as well as fixed networking devices (networking nodes, cloud nodes, access nodes etc.). It utilizes the SDN/NFV programmability as well as the configurability of 5G devices in order to meet the 5G design specifications (e.g. bandwidth, capacity latency).</td>
</tr>
<tr>
<td>• <strong>The Control Plane</strong> is responsible for the control functionality of the network. Realized through a set of controllers and devices that facilitate the creation and destruction of network flows and paths.</td>
<td>• <strong>The business enablement layer</strong> contains all the necessary functions for the 5G converged network in the form of modular architecture building blocks. These blocks, along with configuration parameters, can be evoked from a common repository upon request depending on the use case.</td>
</tr>
<tr>
<td>• <strong>The Application Plane</strong> is responsible for generic network management auditing, and reporting functionalities (e.g., SDN management, monitoring and security). Realized through different network management applications (e.g. Network visualization).</td>
<td>• <strong>The End-2-End (E2E) management and orchestration</strong> entity has access to manage and orchestrate (or coordinate) the above mentioned architectural blocks. In addition, it defines network slices for each use case, interconnects the relevant functions of the network, assigns the proper configuration to meet E2E specifications and maps all these to the network entities of the infrastructure resource layer.</td>
</tr>
<tr>
<td>• <strong>The East/West bound API</strong> is implemented by the different controllers of the SDN and is used to facilitate communications between them.</td>
<td>• <strong>The business application layer</strong> contains applications and service of the 5G network operators or other enterprises that use the network. An interface to the E2E management and orchestration entity can be used to map an application to existing network slices, or to create new slices for the applications.</td>
</tr>
<tr>
<td>• <strong>The Southbound API</strong> is implemented by the different forwarding devices in the SDN to enable the communication between these devices and the controllers of the net-work.</td>
<td></td>
</tr>
<tr>
<td>• <strong>The Northbound API</strong> is implemented by the controllers of the SDN and is used to facilitate the communication between controllers and the network management apps</td>
<td></td>
</tr>
</tbody>
</table>
Activities SDN/5G TTL

- Classification of assets: Mostly for SDN
- Classification of threats: Following ETL taxonomy!
  - SDN
  - Network Virtualization
  - 5G Threats
- Threat Agents classification
- Good practices:
  - Existing mitigation practices
  - Threat mitigation practices under development
- GAP analysis
- Recommendations
  - Technical recommendations
  - Organizational recommendations
Figure 4 - SDN assets threat landscape
SDN/5G Threats

- SDN “specific” threats
- Network Virtualization threats
- 5G/Radio access threats
SDN threats

Figure 5 - Threats of SDN reference architecture
API exploitation: This threat involves exploiting the API of a software component in order to launch different types of further attacks. API exploitation may relate to all the different types of APIs that may be found in an SDN. These include:

- Northbound API (Northbound API exploitation) that facilitates the communication between SDN controllers and SDN applications;
- Southbound API that facilitates the communication between SDN network elements and SDN controllers
- Eastbound/Westbound API that facilitates the communication between SDN controllers

Memory scraping: This threat arises when an attacker scans the physical memory of a software component in order to extract sensitive information that is not authorized to have. Memory scraping can affect components of any layer, this type of threat has been primarily identified for application servers.

Side channel attack: This threat involves extracting information on existing flow rules that are used by network elements. The threat can be realized by exploiting patterns of network operations (e.g. exploiting the time required for establishing a network connection). Side channel attacks is a threat relating to network elements of the data plane.

Data forging: This threat involves compromising an SDN element (e.g., controller, router, switch) in order to forge network data and launch other attacks (e.g., DOS). Data forging is a threat related to components in the data plane and the controller plane

Software/firmware exploits: Involves exploiting vulnerabilities of the software/firmware, in order to cause some malfunction, reduction or disruption of service, eavesdropping of data or destruction/compromising of data. Software/firmware exploits may occur in all layers of the SDN reference architecture.
Taxonomy of SDN Threats

Threats

- Nefarious Activity / Abuse
  - Manipulation of information / Data forging
    - Software/hardware exploits
      - Denial of Service (DoS)
    - Remote SDN application exploitation
      - SDN API exploitation
        - Malicious Software
        - Unauthorized activities
        - Virtualized Operations
- Disasters
  - Natural disasters
    - Environmental disasters
  - Breach of SLAs
    - Breach of legislation
    - Judicial decisions/work orders
  - Abuse of personal data
    - Illicit competition
  - Outages
    - Loss of resources
    - Loss of support services
    - Loss of network connectivity
  - Physical attacks
    - Theft
    - Information exfiltration
    - Unauthorized access
    - Tampering
  - Equipment failure or malfunctions
    - Failure of devices or systems
      - Failure of disruption of common links
      - Failure or disruption of main supply
      - Failure or disruption of service providers
      - Malfunction of equipment
  - Human error
    - Improper use of administrator
    - Maintenance mix-up
    - Data loss
    - Damage caused by third party

Traffic shifting
- Side-channel attack
- Identity spoofing
- Software/hardware exploits
- Memory corruption
- Virtualized Operations
- Traffic sniffing
- Man-in-the-middle
- Interception of information

ENISA TTL SDN/5G | Louis Marinos
Network Virtualization Threats

Threats related to servers running virtualized network functions (virtualized host abuse). Virtualization of functions and their operation on virtual machines (e.g., a server that can be used as a network switch) is a common practice in SDN. Therefore traditional security threats for servers running virtualized network operations such as network monitoring, access control, network management etc. should be considered.

Threats to data centers hosting SDN operations (Data center threats). Many SDN systems are deployed within data centers. Hence, security threats of data centers should be considered, similarly to the server case. Moreover, data servers are using Data Centre Interconnect (DCI) protocols, which may lack authentication and encryption to secure the packet contents. Thus an attacker could create spoofed traffic in such a way that it traverses the DCI links or to create a DoS attack of the DCI connections.

Threats related to virtualization mechanism: (Network Virtualization bypassing). The use of the network between different tenants need to assure that only legitimated traffic enters or leaves a network slice, but also that any switching element checks and enforces the traffic isolation by installing legitimate flow-rules preventing slice trespassing.
User emulation: Adversaries can exploit the wireless medium by mimicking the incumbent signals. Such attacks can be launched by:

- Greedy mobile nodes, mislead other users by transmitting fake incumbent signals in order to lead them to leave a specific band and gain exclusive use of it
- Malicious mobile nodes that to cause Denial of Service (DoS) attacks by mimicking incumbent signals

Spectrum sensing data falsification. The received signal power may enforced to become lower compared to what path loss models have predicted due to transmission features such as signal fading or multipath propagation. This may lead to harmful interference due to undetected primary signals.

MAC layer attack. This category of attacks includes:

- MAC spoofing in which attackers send spurious messages that disrupt the network operation
- Congestion attacks in which attackers flood Common Control Channel in order to cause an extended DoS attack
- Jamming in which adversaries trigger DoS attacks by creating interference at the physical layer.
Recommendations

Technical Recommendations

- **Recommendation 1 (for Network providers):** Mandate encryption and authentication in NBI, SBI and EWBI.
- **Recommendation 2 (for Network providers):** Identify and monitor exposed functionalities of SDN controllers.
- **Recommendation 3 (for Network and Service providers):** Control and monitor running application resources.
- **Recommendation 6 (for Developers):** Sandbox-ing, Application Isolation.
Recommendations

Organizational Recommendations

• Recommendation 7 (for Service providers): Develop incident response capabilities and information sharing practices among telecom operators.

• Recommendation 8 (for Administrators): Keep systems up to date.

• Recommendation 9 (for Network and Service providers): Use adequate security methods.
Challenges on 5G security

- Standardization challenge
- Trust model and Identity Management
- 5G radio network security
- Flexible and scalable security architecture
- Energy-efficient security
- Cloud security
Conclusions

- There is a long way for 5G
- Must be prepared for old and new threats: Different and new layers implies new attack surfaces
- There is a good opportunity to implement security by design
- SDN/NFV is a key actor to improve security on 5G
Thank you for your attention

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu