Threat Modelling for 5G networks

Bernardo Santos
OsloMet – Oslo Metropolitan University
Oslo, Norway
bersan@oslomet.no

Luis Barriga
Ericsson AB
Stockholm, Sweden
luis.barriga@ericsson.com

Bruno Dzogovic
OsloMet – Oslo Metropolitan University
Oslo, Norway
bruno.dzogovic@oslomet.no

Ismail Hassan
OsloMet – Oslo Metropolitan University
Oslo, Norway
ismail@oslomet.no

Boning Feng
OsloMet – Oslo Metropolitan University
Oslo, Norway
boningf@oslomet.no

Niels Jacot
Wolffia AS
Oulu, Finland
n.jacot@wolffia.net

Van Thuan Do
Wolffia AS
Oslo, Norway
vt.do@wolffia.no

Thanh Van Do
Telenor Research &
OsloMet – Oslo Metropolitan University
Fornebu, Norway
thanh-van.do@telenor.no

Abstract*—The new fifth generation (5G) mobile cellular network brings enhanced mobile broadband, massive machine type communication (e.g. IoT), critical machine type communication and fixed wireless access and will accommodate new services and applications such as augmented reality, and seamless streaming to all. 5G will boost security with encrypted data, segmented networks (network slices), enhanced privacy, and user authentication, but the 5G success may also attract attackers to look for vulnerabilities, exploits or eavesdropping. The increase in connected devices creates more targets, and larger attack surfaces, hence attacks on vital connected systems could become more chaotic and consequential. The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework attempts to provide a comprehensive overview of the methods (Techniques) by which an attacker can achieve various operational objectives (Tactics). However, some techniques may not be included in the MITRE ATT&CK matrices. This paper proposes to enhance the ATT&CK framework with Adversarial Tactics and Techniques catered for the mobile network infrastructure – CONCORDIA Mobile Threat Modeling Framework (CMTMF).

***Keywords*—mobile security, cyber security, threat modelling, threat intelligence**

I. Introduction

With the global digital transformation accelerated by the pandemic, cyber-attacks on governmental and commercial organizations and also private individuals increase both in terms of number and level of sophistication. Signature-based intrusion detection using Indications of Compromise (IoCs) is no longer sufficient to provide protection against *Zero-Day* attacks or *Advanced Persistent Threats* (APTs). In fact, IoCs are forensic data gathered and shared from systems that have been breached and are hence less useful in the detection of brand new and sophisticated cyber-attacks. To complement IoCs, it is essential to understand the behavior of the attacker i.e., the actor responsible for the attack, its tactics, techniques and procedures (TTPs). Consequently, a sound and efficient Threat Modelling Framework is urgently demanded, especially for virtualized 5G networks.

The MITRE ATT&CK [1] is currently one of the popular threat modelling frameworks which provides solid fundaments for the description and analysis of cyber threats of enterprises networks and mobile devices. Unfortunately, it does not address neither 5G networks nor mobile networks in general.

Indeed, due to the softwarerization of mobile networks and their reliance on Web technologies, 5G networks are not only subject to the same cyber threats as regular enterprise networks but are also exposed to the ones brought by its capability of providing connectivity to billions of IoT devices ranging from primitive sensors to advanced medical equipment requiring ultra-reliable and low-latency connections. Potential attackers to 5G networks have different behaviors, tactics and techniques that require extensions to the current MITRE ATT&CK framework. The BHADRA framework [9] was the first attempt to extend the MITRE ATT&CK framework for mobile networks which emphasizes the need for modelling threats in mobile networks but is unfortunately too simple and incompatible with the mainstream MITRE ATT&CK framework.

To address this urgent need in the mobile networks, especially 5G networks this work proposes and develops a CONCORDIA Mobile Modelling Framework (CMTMF), which is a compatible combination of the enterprise, mobile and ICS (Industrial Control Systems) matrices of the MITRE ATT&CK framework. The work also includes the implementation of the CMTMF in MISP (Malware Information Sharing Platform) [10], which is a open-source threat intelligence platform.

II. Threats in 5G Networks

Threats in 5G can be classified into two dimensions. In the first dimension, there are threats on the mobile network itself. In the second dimension, all the threats which are related to the virtualization of the mobile networks are gathered i.e., issues related to the hosting of virtual Network Functions (vNFs) in the cloud. Since the threats in the second dimension can be adequately modelled using the MITRE ATT&CK Enterprise and Cloud matrices, this work focuses only on threats in the first dimension.

At high level, a 5G network is exposed at the entry points as shown in Figure 1:

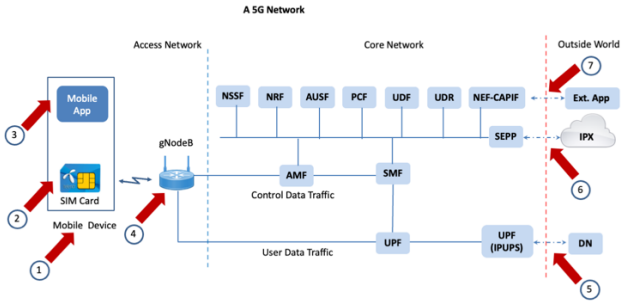

Figure 1 Cyber-attack entry points for a 5G network

© 2022 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

DOI: https://doi.org/10.1109/IWCMC55113.2022.9825149

- **Entry Point 1 - The mobile device:** It may no longer be a common smartphone or a primitive IoT device but a hostile supercomputer that can inject dirty data into the network. Some mobile phones can allow remote request to update the device configuration e.g., OMA CP (Open Mobile Alliance Configuration Provisioning) and letting attackers to take over the phone.
- **Entry Point 2 - The SIM Card:** Although being a tamper resistant module, a SIM card may still have unknown vulnerabilities that can be exploited to change the configuration of the mobile phone, e.g., change of Access Point Name (APN).
- **Entry Point 3 - The mobile app:** A lot of mobile applications, even coming from trustworthy stores, can expose user data and compromise the user equipment that is connected to the mobile network.
- **Entry Point 4** - The gNodeB: As the gateway between devices and the 5G network, attackers can use the open interfaces from a gNodeB to attack the network, including the radio baseband.
- **Entry Point 5 - The IPUPS:** the Inter-PLMN UP Security at the perimeter of the Public Land Mobile Network (PLMN) for protecting user plane messages.
- **Entry Point 6 - The SEPP:** Acting as a security proxy for all signaling traffic between operators (roaming)
    - Provides security for the control plane messages;
    - It is assumed that intermediate IPX providers are trustworthy;
- **Entry Point 7 – The Network Exposure Function (NEF) - CAPIF:** aimed at providing a common and unified (API) framework to allow an agreement between available network functions.
    - Interfaces with Data networks (DN) sufficiently protected;
    - Interfaces with other mobile networks have been a weakness of the mobile networks;
    - Interfaces towards external applications are limited.

III. State of the Art in Threat Modelling Framework

A. Definition of Threat Modelling

Threat modelling is the activity aiming at identifying, understanding and making simple descriptions or models of the potential threats and attack vectors that a system could be exposed for such that risk analyses, detection methods, countermeasures, and mitigation strategies can be developed. A threat modeling framework usually includes five components, namely threat intelligence, asset identification, mitigation capabilities, risk assessment and threat mapping, but may have different focuses as follows:

- Asset-centric threat modelling frameworks focus on the assets of the target system
- Attack-centric threat modelling framework focus on the attackers and attacks
- System-centric threat modelling framework focus on target system

It will be shown later that the **attack-centric approach** is most appropriate for the threat modelling of mobile networks and the MITRE ATT&CK is selected as fundament for this work.

B. BHADRA Framework

In order to provide a more common ground for threat modeling for mobile infrastructures, the authors in [9] developed the *BHADRA* framework, a domain-specific format to model attacks given its phases or stages, which are mounting, execution and results. Aligned with the premises of MITRE ATT&CK, it consists of 47 techniques to describe the attack's life cycle, regardless of the target in a mobile network.

C. MITRE ATT&CK

"MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target."[1]

Established in 2010, the Fort Meade Experiment (FMX) research facility allowed researchers to use MITRE's tools with the purpose of how to better detect threats [1]. The type of tests and activities done in that environment were always done under the assumption that a breach in their network or infrastructure has happened and the researchers were to document all the detected threats and come up with possible ways to impede a widespread effect or to protect the infrastructure from the tested exploits.

1) Tactics

The "**Why**" in Threat Modelling, a tactic aims to explain the reason as an attacker performs a certain action [1]. Its definition will establish which techniques should be grouped into it or that are under the tactic's spectrum.

2) Techniques

Techniques showcase the "**How**" in an action performed by an attacker [1]. It provides more detailed information regarding the action taken depending on the chosen target, which can be link as to "**What**" has been done. As mentioned above, there are multiple techniques that can be group under the same tactic.

3) Sub-Techniques

Some techniques can be valid for multiple tactics and can have different variations given the media that they are being analyzed (e.g., network vs. mobile), hence sub-techniques [2] allow us to specify at a deeper level an action taken by an attacker.

4) Procedures

Procedures [2] describe the implementations used for each described technique or sub-technique that an attacker has used.

5) Mitigations

Mitigations are the countermeasures [2] aimed to prevent the tactics used by an attacker. They are considered the "What to do" when facing a possible threat.

D. MITRE ATT&CK Matrices

1) Enterprise

The first knowledge base (and considered to be the basis for other existing frameworks) coming from MITRE ATT&CK, it aims to document adversarial behaviors that target enterprise infrastructures (e.g., Windows, Network, among others). In its latest version (November 2021), this framework has 218 techniques, which some of them are multi-level [3][4].

2) Mobile

The Mobile framework aims to document and describe effects given an attack that has targeted mobile phones, and mostly the ones that are supported by the *iOS* or *Android* operating systems. Its latest version (November 2021) has 111 techniques, where the focus is more about data or software compromise. It is worth mentioning that possible documented effects that occurred in the network infrastructure are addressed in a sub or separate framework [5].

3) ICS

The focus of this knowledge base is to provide ways to describe actions that were afflicted in an Industrial Control Systems (ICS) network, in which IoT devices can be a part of. It is comprised of 88 techniques (as of October 2021) that illustrate the effects provoked by an attack, from a data or software compromise to rendering equipment useless [6][7].

4) Cloud

A sub-matrix from the Enterprise knowledge base, Cloud [8] has its focus on documenting actions that are done in a cloud-based environment. Given that 5G networks have a strong cloud component, the techniques linked to this environment are also quite relevant.

There are ATT&CK matrices for the enterprise and mobile device domains, but there is none for Telecom networks. We believe that for the Telco domain an ATT&CK matrix could be useful in several ways:

- **A new class of adversaries** – There are different types of adversaries. A user only needs a rooted phone and a SIM card to get access to a mobile network and start attacking it. Adversaries don't always need a phone and can just develop radio network equipment to conduct radio-level attacks. A mobile operator in a jurisdiction with no business/legal can abuse the interconnection networks to conduct attacks or fraud. As mobile networks are part of most countries' national infrastructure, some nation states are also potential adversaries. By modelling the behavior of such adversaries, it is possible to design the proper detection and mitigation measures.
- **Extrapolating adversarial behavior** – while understanding the adversary helps in defending against known attacks, the matrix can be used as a baseline help in developing new possible adversarial behavior.
- **Penetration testing** – A telco matrix can guide operators to simulate attacks and assess the robustness of their networks identifying vulnerabilities.
- **Risk assessment** – a telco matrix can be used during the risk assessment process that operators must conduct regularly as part of the operations. Operators can assess how they have managed the different threats in the Telco matrix.
- **Sharing and enriching threat models** – by properly describing the complete attack behavior, with the necessary contextualization, enrichment and defenses, operators can exchange this information across the Telco community and contribute to the overall security of the global telco industry.

We noticed that when attempting to describe threats to the Telco domain using the available enterprise and mobile device ATT&CK matrices these were partially suitable. Some of the techniques and tactics were applicable, but there were also differences as mobile networks and enterprise networks have totally different trust and threat models. Also, the mobile device matrix mainly covers the device side and not the mobile infrastructure. The Telco threat landscape is also evolving, and the challenge is to design an adequate ATT&CK modelling framework that can capture the complex interaction between new type of devices, new 5G network technologies, new supported use vertical cases and upcoming generation of mobile networks.

To show the complexity of modelling a threat in Telco we will show an example of a potential threat from the cellular IoT domain as described in the 3GPP TR 33.861 where it is mentioned that low-end low-security cellular IoT devices are likely to be massively deployed, and they could be compromised and used for DDoS and flooding attacks disrupting mobile network services.

To model the adversarial behavior of such attacks the following tactics and techniques would be employed:

- **Preparation –** adversaries would do some homework identifying cellular vulnerable IoT devices that use non-secure software, OS or hardware components.
- **Resource Development** – adversaries develop or obtain tools to attack IoT devices, deploying C&C centers, keeping a library of exploits per device, port scanners, automated password guessing tools, collecting commonly used passwords in IoT devices or exploits to enter the device. Even IMSI catchers can be used to identify devices or false base stations to attract devices to camp and being scanned.
- **Reconnaissance** – adversaries conduct market analysis of the penetration of vulnerable devices in different geographic areas looking for high-density deployments.
- **Initial access –** adversaries launch cellular scanners that look for vulnerable devices that once compromised are listed as candidate botnets. The adversary makes of profile of the device CPU architecture, OS and software.
- **Execution –**adversaries communicate with a C&C center via the IoT device to download botnet code turning the device into botnets.
- **Persistence & Defense Evasion –** once the IoT device has effectively become a botnet, the botnet makes a "hardening", removing any IoT software and services that can disturb its work. The botnet also removes any

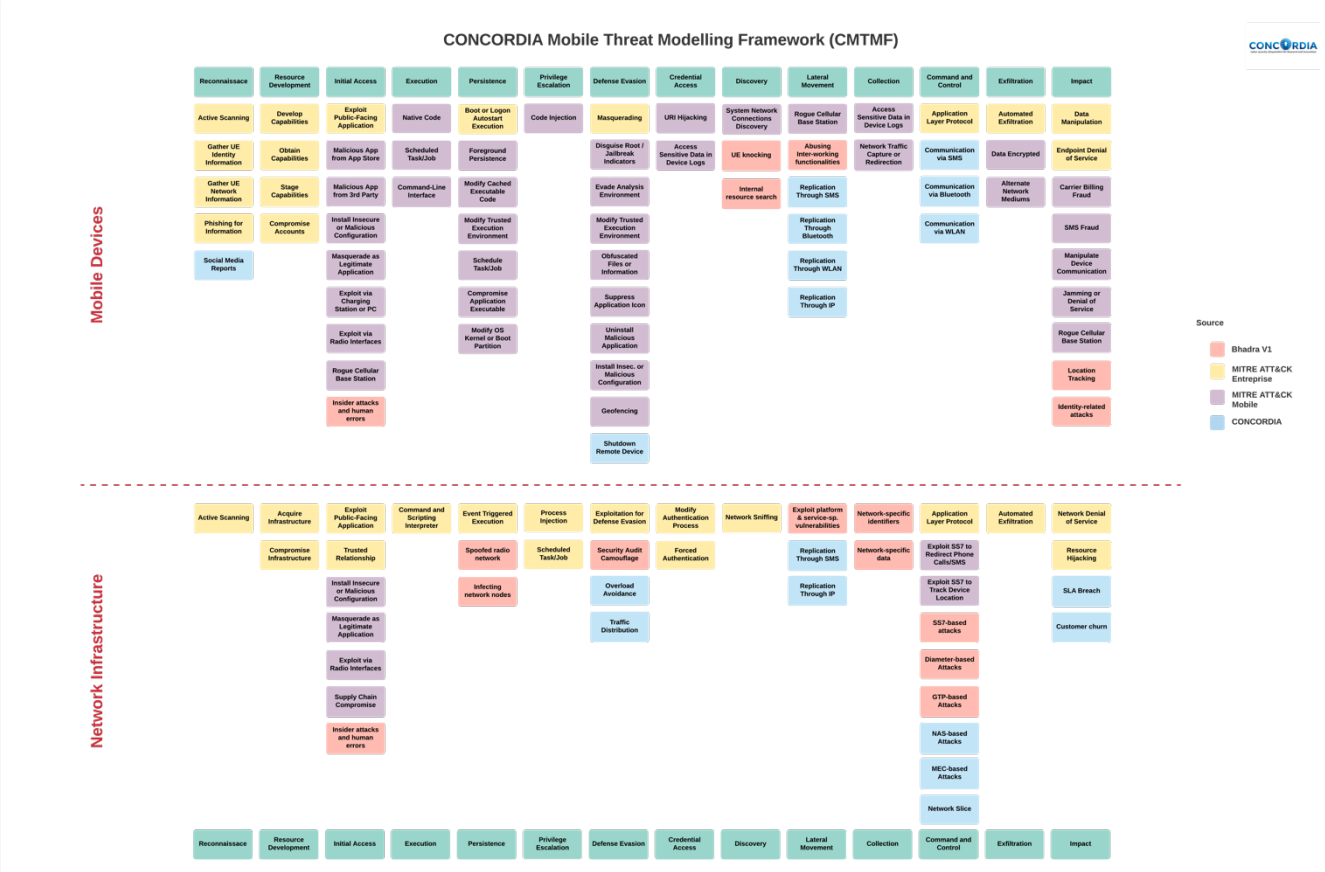

Figure 2 The CONCORDIA Mobile Threat Modelling Framework

possible defense mechanisms or even competing botnets. The IoT device is now under full control of the C&C center.

- **Discovery –** botnets start looking for additional IoT devices in the geo-location neighborhood repeating the initial access techniques. IoT devices report their geo-location.
- **Command & Control**– the botnet uses encrypted communications, proxies, URLs, SMS to hide its contact with the C&C centers. The C&C centers also change DNS names and IP addresses to avoid detection. Security-by-obscurity techniques are also used to keep the hidden communication with the botnets.
- **Impact** – Under the C&C control, and by having the geo-location of all botnets, the adversary can launch targeted geo-location network attacks such as DDoS or flooding.

As it can be seen from the attack description, while the tactics and some of the techniques resemble the ones used in enterprise and mobile, there is a need for new techniques that are mobile network specific. Even the sequence of tactics is a combination of network and device ones. Based on this and other mobile-specific use cases, we have developed a new ATT&CK threat modelling framework.

IV. CONCORDIA MOBILE THREAT MODELLING FRAMEWORK

The Concordia matrix, as shown in Figure 2, is aligned with the MITRE Enterprise matrix and has 14 tactics. The techniques from the mobile matrix represented by purple boxes are merged with the one of the Enterprise matrices in yellow boxes. The CMTMF includes also the techniques proposed by the BHADRA framework represented by red boxes. Since it is not sufficient with the current techniques, we have proposed additional CONCORDIA techniques represented by blue boxes. This is the first iteration of this framework and its intention is to adapt and grow as we see the need to accommodate more techniques as more attacks become known. Also, as we continuously update our framework, our intent is to replace all techniques coming from the first iteration from BHADRA with our own.

However, and unlike MITRE ATT&CK, no tactic is unique, instead we document an attack by **phases** or **stages**, for an attack in a mobile network can be a sum of events that are documented by the existing techniques from a specific tactic in different occasions.

An attack in mobile networks can be recursive as it can spread to multiple devices, so we use **loops** to showcase this behavior. This will allow operators to see the true impact of an incoming or detected and in progress attack.

When using CMTMF to model an attack on the mobile network, the aim is to reflect which effects it will have/has had on **devices** as well as and alongside with the **operator's network infrastructure**, giving a unified view of the documented chain of events.

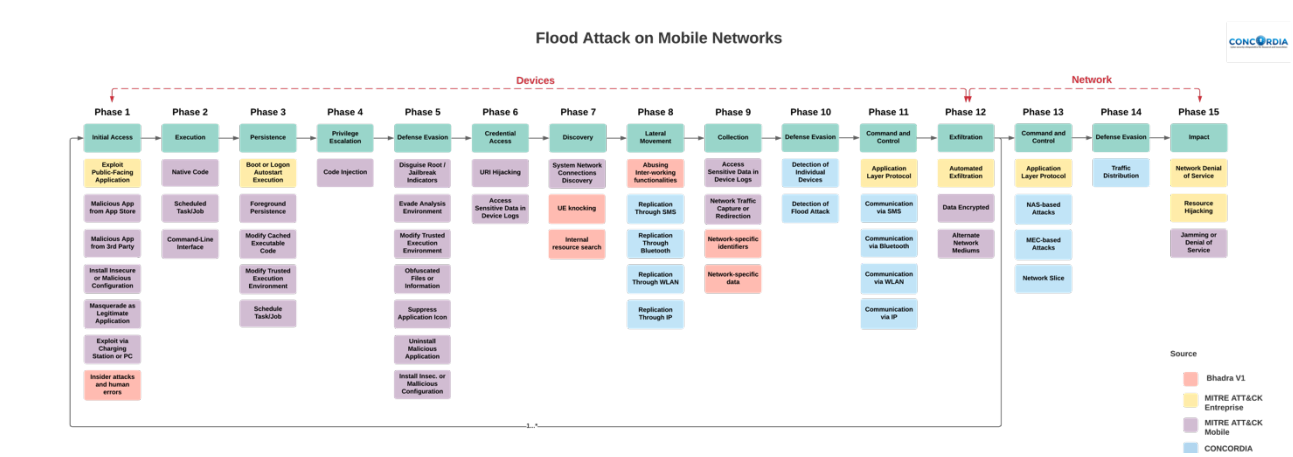

Figure 3 Flood attack modelled with CMTMF

V. Modelling Attacks with CMTMF

To illustrate the use of the CMTMF let us consider a flood attack by IoT devices on the 5G network. So far, there is no such attack yet because 5G is still at earlier deployment stage. However, with the emergence of billion IoT devices in the mobile network, flood attacks by infected IoT devices constitute one of the biggest threats on 5G networks and it is essential to model, analyze and find measures to prevent it.

As shown in Figure 3, a flood attack starts on the devices. The attacker will try to infect and take over control of a large number of IoT devices that is needed for the attack. This Device stage consists of 12 phases: 1. Initial Access – 2. Execution – 3. Persistence – 4. Privilege Escalation – 5. Defense Evasion – 6. Credential Access – 7. Discovery – 8. Lateral Movement – 9. Collection – 10. Defense Evasion – 11. Command and Control – 12. Exfiltration. This stage is repeating multiple times until the number of hijacked devices reaches a certain number and the flood attack can now be launched. The Network stage can now begin and consists of 3 phases: 13. Command and Control – 14. Defense Evasion – 15. Impact.

As mentioned earlier, CMTMF describes and documents an attack by phases, and as it is shown in Figure 3, it is worth emphasizing that the Defense Evasion Tactic is present twice in the Device stage and once in the Network stage as well as the Command and Control tactic, that is represented once in the Device stage and again in the Network stage.

VI. Integration in Misp

One important task is the implementation of the CMTMF in MISP such that threats on mobile network can be shared in such platform. As of late December 2021, CMTMF is available to all MISP [11] users. This was possible given the close collaboration established with CONCORDIA consortium and CIRCL [12] in Luxembourg.

The process went through migrating CMTMF to the nomenclature used by the platform, which is described by the following:

- **Taxonomy:** *"A taxonomy contains a series of tags that can be used as normal tags in your MISP instance. Tagging is a simple way to attach a classification to an event. In the early version of MISP, tagging was local to an instance. Classification must be globally used to be efficient."[13]*
- **Galaxy:** *"MISP galaxy is a simple method to express a large object called cluster that can be attached to MISP events or attributes. A cluster can be composed of one or more elements. Elements are expressed as key-values."[14]*
- **Object:** "*MISP objects are containers around contextually linked attributes. They support analysts in grouping related attributes and describing the relations that exist between the data points in a threat event."[15]*
- **Event:** "*MISP events are encapsulations for contextually related information represented as attribute and object."[16]*

The CMTMF, given all its current tactics and techniques is now a MISP galaxy. As we continue to expand and update our framework, further versions will also be available in the MISP platform.

Combining both CMTMF and MISP workflows, when creating an event on MISP, users will have the capability of selecting one or several techniques associated to a tactic, which we now consider as a phase. All relevant information to that phase should be added or extended to that event.

As events/phases are added in MISP, there is a need to establish a link between them so we can see the correlation chain of the documented attack. To that end, we've developed a MISP (meta) object called *concordia-mtmf-intrusion-set* to help determine the phase number (to verify the chain), the name of the attack, the name of the tactic (for the user's reference) and if the phase will trigger a loop, meaning that that the chain established up to that point will repeat itself. All the elements of this object will allow the MISP user to not only see the full chain of events associated with an attack but also compare with other events and/or attacks that have been shared by other partners.

We've also created mockups to propose and introduce some additions to the MISP interface so that CMTMF can be easily accessible, being one of the relevant changes the correlation graph that will showcase the sequence of an attack described by the documented events, which is already available in the latest MISP version and an usage example is shown in Figure 4 .

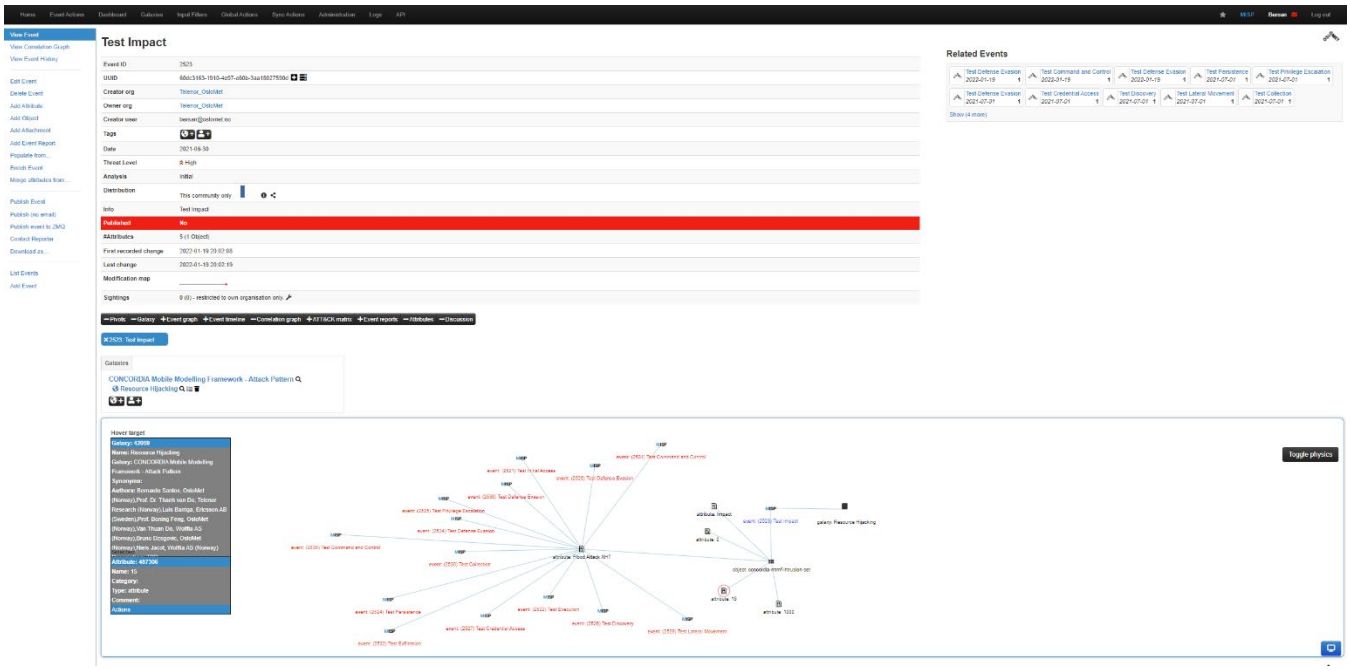

Figure 4: Usage of CMTMF in MISP

VII. Conclusion

The concept of using an end-to-end cyber-attack taxonomy as a reference to gain adversary's perspective, is not new. The Lockheed Martin Cyber Kill Chain is another popular framework to model and understand adversarial behaviors. However, the ATT&CK framework is unique for the ways it drills down into the various attack tactics, techniques, and procedures, suggesting appropriate mitigation strategies and standardizing the language. Therefore, ATT&CK and compatible frameworks like CMTMF facilitate tremendously the sharing of threat intelligence.

The bad actors out there will continue to evolve their methods every single day and attacks across every industry will rise. It is critical to become more resilient to future cyber threats —large-scale data breaches and massive flooding attacks. Those frameworks will also support the development of immediate best practices and long-term strategic plans to mitigate and stabilize cybersecurity risks across the industry, especially the mobile networks.

Acknowledgment

This paper is a result of the H2020 Concordia project (https://www.concordia-h2020.eu) which has received funding from the EU H2020 programme under grant agreement No 830927. The CONCORDIA consortium includes 23 partners from industry and other organizations such as Telenor, Telefonica, Telecom Italia, Ericsson, Siemens, Airbus, etc. and 23 partners from academia such as CODE, university of Twente, OsloMet, etc.

References

[1] Strom, B. E., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). MITRE ATT&CKTM: Design and Philosophy. https://www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy

[2] Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. Sensors, 21(9). https://doi.org/10.3390/s21093267

[3] MITRE ATT&CK Entreprise [Online]. Available: https://attack.mitre.org/matrices/enterprise/

[4] Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2021). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. Software and Systems Modeling. https://doi.org/10.1007/s10270-021-00898-7

[5] MITRE ATT&CK Mobile [Online]. Available: https://attack.mitre.org/matrices/mobile/

[6] Kwon, R., Ashley, T., Castleberry, J., McKenzie, P., & Gupta Gourisetti, S. N. (2020). Cyber threat dictionary using MITRE ATTCK matrix and NIST cybersecurity framework mapping. *2020 Resilience Week, RWS 2020*, *75*, 106–112. https://doi.org/10.1109/RWS50334.2020.9241271

[7] MITRE ATT&CK ICS [Online]. Available: https://collaborate.mitre.org/attackics/index.php/Main_Page

[8] MITRE ATT&CK Cloud [Online]. Available: https://attack.mitre.org/matrices/enterprise/cloud/

[9] Rao, S. P., Holtmanns, S., & Aura, T. (2020). *Threat modeling framework for mobile communication systems*. http://arxiv.org/abs/2005.05110

[10] MISP [Online]. Available: https://www.misp-project.org/

[11] MISP 2.4.152 Release. Available: https://test.misp.software/2021/12/22/MISP.2.4.152.released.html/ (last accessed: 1 Feb 2022)

[12] CIRCL [Online]. Available: https://circl.lu/

[13] MISP Taxonomy Definition [Online]. Available: https://www.circl.lu/doc/misp/taxonomy/

[14] MISP Galaxy Definition [Online]. Available: https://github.com/MISP/misp-galaxy#:~:text=MISP%20galaxy%20is%20a%20simple,are%20expressed%20as%20key%2Dvalues.

[15] MISP Object Definition [Online]. Available: https://www.misp-project.org/2021/03/17/MISP-Objects-101.html#:~:text=MISP%20objects%20are%20containers%20around,points%20in%20a%20threat%20event.

[16] MISP Event Definition [Online]. Available: https://www.circl.lu/doc/misp/GLOSSARY.html