TOWARDS DYNAMIC THREAT MODELLING IN 5G CORE NETWORKS BASED ON MITRE ATTACK - Notes

Cameron Noakes

November 2021

0.1 Sentence Overview

Early stage 5G networks incorporating the use of the Mitre Attack framework with a potential sub-framework MITRE for 5GCN, exploitation of network functions NFV and SDN.

1 Introduction - Notes

The paper introduction details the definition of APT threats by exclaiming the statement of APTs being the "threat to the cyber security of modern technology".

The paper details how due to the increase in digital transformation of advanced persistent threats, they begun to move more towards targeted isolated environments from the internet like critical infrastructure and vendor supply chains. Due to this change cyber security professionals now need to reassess their methodology and alter the approach towards threat modelling and risk assessments.

Briefly explains the use of 5G networks and what the issuing companies wish to bring which is a service-rich technology for various use cases. Describes how the new 5G networks introduce new cyber challenges from new emerging technologies.

Breakdown and explanation of common threat modelling situations are given, how a high level abstraction of the target system, sub-systems and interfaces is initialised to profile potential attackers and estimate their end objectives. This allows a complete catalogue of possible threats and a list of security controls to address the issues and mitigate them.

Most threat modelling situations and models are often generating static representations, since 5G networks like 5GCN it can be difficult to apply a threat model to a 5G network scenario due to them being effective, resilient and dynamic (constantly evolving).

This is where the Mitre Attack Framework comes in, due to most threat models being static and unable to be applied to 5G dynamic network modelling scenarios, the Mitre Attack Framework is a flexible, dynamic threat model for malleable systems and enterprise networks. Due to its tactics, techniques and procedures (TTPs) it allows neutral environment threat modelling in which is dynamic for security controls.

The introduction continues to delineate the proposed solution for this article paper, the proposed solution is that an extension (or bi-product) of the Mitre Attack Framework should allow to incorporate a set of 5G adversarial techniques and to detail discussions for the extension to be used for modelling threats.

The paper also illustrates how the Mitre Attack Framework can be able to systematically identify 5GCN infrastructure to assess risk before and after intrusion to help aid and support threat modelling and risk assessments.

2 Background

Additional information is given regarding the Mitre Attack Framework and how it identities adversarial behaviour and methodology which form specific attacks expressed as graphs to demonstrate multi-step attacks.

Mitre Attack Framework for threat modelling is compared to high level threat models such as STRIDE and also low level threat models similar to CVSS due to the Mitre Attack Framework being considered a mid-level abstraction. The framework is considered to also be proactive event-driven and is constantly updated as new behaviours are observed within the industry for cyber threats.

In this paper, the researchers discuss the study of how to extend Mitre Attack Framework for TTP knowledge base for 5G networks. Acknowledgement of a similar framework is mentioned, the 'Bahdra Framework' which is a domain specific threat modelling framework for telecommunications which ideally could be a good fit for 5GCN networks, however the researchers wish to develop their own proposed solution to better fit the specific nature of 5G networks such as a heavier focus on data exfiltration which is prominent in 5G networks and including techniques which span across various tactic groups.

3 5G Threats

the researchers have completed a literature review in order to relate to the new 5GCN networks and technology.

The 5G network functions are discussed to have been implemented in the virtual layer through 'Network Function Virtualisation (NFV)'. The SDN service is used to provide a programmable interface for network management.

If a shift of cloud based services for deployment would result in another risk as a new attack vector is placed onto the internet for adversarial attackers. Dynamic VNF deployment also could potentially lead to configuration errors which would introduce vulnerabilities within the environment.

Speaks highly about low level services and functions in which 5GCN networks would incorporate but out of scope for this white paper due to its complexity and relevancy.

With network functions (NF) becoming exposed, there is a risk that they could be targeted by adversarial attackers with experience attacking these technologies. Exploited network functions could potentially lead to serious compromise such as unauthorised access to data repositories.

4 Mitre Attack in 5G

Overview of where the Mitre Attack Framework is implemented mostly within the industry which is commonly enterprise networks, Industrial Control Systems (ICS) and mobile devices.

However there is a specific related framework called 'Mitre for ICS' which is uniquely used to identify risks and threats within ICS environments this section did not mention this and could be a better solution rather than using the generic framework applied to a specific industry not like others.

There is gaps in literature and threats in the Mitre Attack Framework for specific 5G network related network functions, much to the same affect as ICS environments needed a framework of their own based on the Mitre Attack Framework, it is wise to develop one for each specific niche that is not enterprise environments to better relate to the provided environment and help reduce risk and mitigate vulnerabilities more effectively. This is a detailed reason for the researchers proposing an alternate solution for the Mitre Attack Framework, so it can be implemented and adapted for the specific use of targeting 5GCN networks, since the Mitre Attack Framework does not account for 5G related features such as SDN,NFV and network slicing.

5 5GCN Tactics, Techniques and Procedures (TTP) Identification

The section on 5GCN identification initialises with an opening statement of how the Mitre Attack Framework identified eight main advance persistent threat (APT) groups with attacks for telecommunication networks. Which are listed to be: (APT19, APT39, APT41, Deep Panda, MuddyWater, OilRig, Soft Cell and Thrip).

The proposed solution is discussed again for how the Mitre Attack Framework should expand the matrix for cloud infrastructure and also include new techniques to incorporate new technologies such as SDN and NFV for 5GCN networks.

6 Pre-Intrusion

The opening paragraph details how there are several, specific access points that could act as attack vectors for adversarial entities. The implemented network functions (NFs) are often able to be reached by RESTful APIs, if certain APIs are exposed to the internet, this would create a new attack vector for 5GCN network intrusion.

7 Post-Intrusion

This section speaks about how attackers can laterally move through an enterprise network evading IDS systems. The opening paragraph details key sections of what is covered under this title from persistence to data exfiltration (aka 'Collection' as it is explained).

Descriptive continuation of the paragraph outlines a 5GCN network attack on network functions (NFs) that deal with image processing and container technology which would be present from a successful supply chain compromisation. This described attack can be categorised under the persistence and defense evasion sections.

This example attack on 5GCN network functions is one example of many that could lead to further compromised systems, in the previous example being that of if the threat actor could break out of the container can move laterally around the network, compromising further devices.

8 Threat Actor Objectives

The opening description outlines that the objectives of an attacker mean the overall goal of the executed attacks which are categorised within the Mitre Attack Framework as data exfiltration (previously known in the paper as collection) and impact techniques.

The researchers explain how an amendment to the framework for 5GCN network infrastructure attacks could outline potential, specific 5G risks and threats.

Elaboration of impact is given being examples such as abuse of lawful intercept function, data modification and charging and loss of security and controls.

9 Mapping attacker techniques to 5GCN

Explains how the Mitre Attack Framework is a mid-level abstraction for adversarial threat modelling which provides more details and has a heavier focus on security monitoring for detection and information regarding how to mitigate the risks and potential threats.

For this mapping to take place the researchers outline how they utilise the mid-level abstraction approach from Mitre and connect the techniques of Mitre Attack Framework to the technologies of the 5GCN network infrastructure.

The researchers take into account that the 5G network is dynamic, various deployment strategies and are aware that the network architecture and infrastructure can change at any given time.

Acknowledgement of if any new network functions are deployed, they will have the same security as the other network functions therefore, allowing a threat model that can be applied to asset types and still address threats to certain new technologies outlined in the 5G network.

10 Multi-Stage Attack Modelling with 5GCN TTPs

This section covers how the threat modelling developed from the Mitre Attack Framework can be demonstrated for 5G networks to model an advance persistent threat (APT). A description about how APTs are broken down into smaller steps (decomposition) in order to relate each step to a tactic in the Mitre Attack Framework matrix.

Even if the defenses cannot prevent all APTs, it could still prevent some of the steps leading to a reduced risk and a minimised impact and attacker success rate.

11 Research Gaps and Questions

The researchers could have potentially acknowledged there being an 'Attack for ICS' which would have worked well to allow the reader to understand the proposed solution in easier steps due to one already being created for a specific purpose.

12 What problem does this solve?

Due to the nature of 5G networks being relatively new, this created a problem to be solved that of how 5G networks care beginning to be exploited and attacked by adversarial attackers and due to the new technologies, don't have the best security implemented to prevent such attacks, this paper proposed a solution in order to deal with this problem.

13 How do they solve it?

The researchers solve an issue that due to 5GCN networks being new and with new technologies that are open to attackers, there will be a proposed solution of another framework based on the Mitre Attack Framework in order to better relate to 5GCN networks and infrastructure in order to better protect them and reduce the APTs and attacker success rate.

14 How do they assess it?

It is difficult to assess new technology due to there being only limited resources and security assessments out there, which does make the paper exploratory and new in the industry, impacting the research provided.

A limitation that is mentioned is how the paper and proposed solution lack real world data analytics due to 5GCN networks being new.

15 Conclusion - Notes

A conclusion was explained of how the Mitre Attack Framework proposed as a suitable framework for threat modelling and due to the dynamic and new tech that 5GCN networks use that an extension of the current framework is proposed in order to better secure 5G networks. This was concluded by the study and explanations of how Mitre prevents APTs and but mainly for enterprise networks, not for specific industries or technologies like ICS, Cloud, 5G and alike.