REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
	Conference Paper	

4. TITLE AND SUBTITLE

Threat framework for 5G cellular communications

5a. CONTRACT NUMBER

W56KGU-18-D-0004

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Michaela Vanderveen

5d. PROJECT NUMBER

100927.10.100.K10P.5S0

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

PRS-22-1977

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

DoD CIO

10. SPONSOR/MONITOR'S ACRONYM(S)

DoD CIO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

Preprint to MILCOM 2022. https://edas.info/web/milcom2022/program.html

14. ABSTRACT

Even though 5G is generally viewed as more secure than previous generations 5G incorporates Internet technologies, which increase the attack surface. In addition, the much larger number of devices connecting, and the new types of such devices also raise new security concerns. The urgency of protecting these networks is increased as 5G is incorporated into human safety critical infrastructure and military establishments. This paper introduces FiGHT- Five G Hierarchy of Threats, a framework of adversarial tactics and techniques applicable to the 5G system, similar to that of MITRE ATT&CK.

15. SUBJECT TERMS

Computer Security; Wireless Communications; threat model; security management; 5G

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Susan Carpenito
				7	19b. TELEPHONE NUMBER *(Include area code)* 781-271-7646

Threat framework for 5G cellular communications

Michaela Vanderveen
Cyber Solutions Innovation Center
MITRE
McLean, VA
ORCID: 0000-0002-5315-2775

***Abstract*—5G networks are rapidly gaining traction as the technology of choice for not only traditional cellular networks, but also new verticals such as business, industrial and military deployments. The complexity of 5G as a system of systems poses new security challenges. Even though 5G is generally viewed as more secure than previous generations such as 4G (LTE), 5G incorporates Internet technologies (e.g., service-based architectures, cloud services, virtualization), which increase the attack surface. In addition, the much larger number of devices connecting, and the new types of such devices (e.g., affecting human safety) also raise new security concerns. The urgency of protecting these networks is increased as 5G is incorporated into human safety critical infrastructure and military establishments. This paper introduces FiGHT- Five G Hierarchy of Threats, a framework of adversarial tactics and techniques applicable to the 5G system, similar to that of MITRE ATT&CK.**

Keywords—threat model, 5G, security management.

I. Introduction

5G networks are rapidly gaining traction as the technology of choice for not only traditional cellular networks, but also new verticals such as business environments, industrial networks/factories, military deployments, critical infrastructure monitoring and uncrewed aerial vehicle (UAV).

5G is a system of systems, and its complexity due in part to the incorporation of Internet technologies (service-based architecture, cloud services, virtualization, etc.) poses new security challenges. Other challenges are due to the devices accessing the cellular network: the much larger number of relatively simple devices that connect (like Internet of Things devices, e.g., smart city sensors), or safety-bound devices (e.g., vehicles, medical wearable devices). All of these types of devices involve no human users. Invariably, new designs come with new risks.

Recent events have shown how telecommunications networks can be weaponized; since they are interconnected globally, and are also used to connect critical infrastructure within a country. For example, state-level adversaries used telecommunication networks to enhance traditional warfare (e.g., gather intelligence about user and device location).

On the positive side, telecommunication networks, especially 5G, are well suited to enable efficient and secure expeditionary and other small scale military deployments, as well as support larger, more permanent deployments in joint armed force bases.

From all these considerations of the human safety factors, it is clear there is a critical need to protect and increase the cyber-resilience of the 5G networks especially as they are used in tactical environments, but also to connect critical infrastructure. The protection of the 5G networks involves ensuring confidentiality, integrity, and availability of communication between devices and networks.

It is well accepted in the cybersecurity community that system defense design should be threat-informed. That is, to achieve the goal of detecting, mitigating, and protecting against cyber-attacks, one must develop a good understanding of the various adversaries' tactics and techniques. To this end, this paper introduces FiGHT™ – Five G Hierarchy of Threats, a framework of adversarial tactics and techniques applicable to the 5G system, covering its sub-system aspects.

II. Related Works

There exist a few threat frameworks applicable to at least some components of telecommunications networks: MITRE ATT&CK® [1] is a publicly available knowledge base of disclosed tactics, techniques and procedures (TTPs). A comprehensive survey of threats and security measures applicable to 5G was published by the European Union Agency for Cybersecurity's (ENISA) [2]. One of the first attempts at a threat framework customized for the telecommunications world, focused on earlier generations is also known as "the Bhadra framework" [3]. A more recent, 5G new technology focused paper on threat modeling was published in [4].

As for standards development organizations (SDOs), the GSM Association (GSMA), an international forum of telecom operators and their vendors, set forth several documents containing known threats to various aspects of the cellular systems [5]. O-RAN Alliance formed a special Security Focus Group (SFG) last year and published a Security Threat Modeling and Remediation Analysis document. Finally, we note that 3GPP (the Third Generation Partnership Project), the international SDO that outputs the specifications for 5G, also produced several study items and technical specifications which contain threats to various network components (see e.g. [6],[7]). There is also a substantive body of published literature on attacks – theoretical mainly – on 5G system components, and at least one blog article [8] highlighting the need for threat frameworks for telecom networks. With the exception of ATT&CK, none of the above are easily applied in operational environments, hence the need for a 5G threat framework.

Funding for this project is provided by Department of Defense (DOD) Office of the Undersecretary of Defense, Research and Engineering (OUSD R&E), as part of the DoD 5G Initiative.

III. Methodology

Threat modeling is the process of identifying known or potential threats to a system, to better enable defenders to plan and react to these threats. Some of the use cases for defenders leveraging a model can include defining and implementing detections and mitigations, emulating adversary activity to test current defenses, and enhancing architectures and designs to close vulnerabilities that could be leveraged by adversaries. Many threat modeling approaches are in use today: attack trees, MITRE ATT&CK®, Microsoft STRIDE, and the Lockheed Martin Cyber Kill-Chain®, to name a few.

Threat modeling in the style of ATT&CK decomposes a given attack into atomic adversary behaviors, which are called Techniques. Each Technique fits under one or more Tactics, which represent why an adversary would perform a given behavior. Tactics can be viewed as short-term objectives of the adversary – e.g., credential access, privilege escalation, impact, etc. Each Technique can also have one or more Sub-Techniques. While a Technique describes a given, atomic adversary behavior, Sub-Techniques specify more precisely how the adversary is achieving the Technique, in context of a given technology, system, and so forth. A key tenant of this model is also that it is developed from the viewpoint of the adversary.

In the description below, by "existing (sub)technique" we mean a technique or sub-technique that is already part of ATT&CK, either Enterprise or Mobile matrices.

Our methodology involves six steps (Fig. 1). First, we collect known threats or attack descriptions as found via review of existing publications. Unlike in ATT&CK, the candidate 5G threats do not need to have been observed "in the wild" and conducted by real adversaries in actual breaches, but can instead be theoretical or a validated proof of concept that the methodology works in practice. Therefore, the sources can be research papers or even blog articles. In addition, some threats can be inferred from the specifications, once the adversarial frame of mind is applied, e.g. abuse of legitimate signaling by a compromised network function. It is important to note that FiGHT will document real-world adversary activity if observed. However, due to the current limited deployment of 5G systems, such observations are exceedingly rare to non-existent.

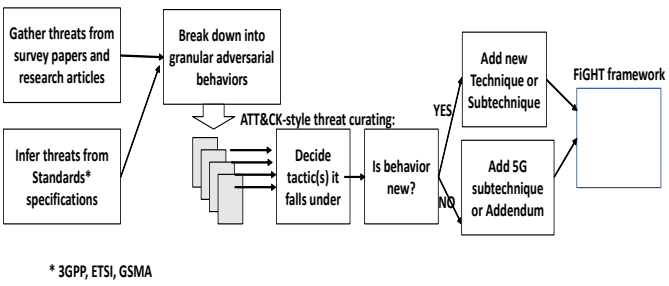

Fig. 1. Methodology of threat framework construction

Second, the attack is broken down into atomic adversarial behaviors, also referred to here as (sub)techniques. For example, a data manipulation attack over the air interface may be decomposed in: 1) deploying a fake base station 2) bidding-down a UE device to 3G or 4G, 3) exploiting the lack of user plane data integrity protection, and 4) readdressing the DNS request to go to an adversary-controlled DNS server. Notably, each threat is described at a mid-level of abstraction like ATT&CK TTPs..

Third, for each such identified behavior, the tactic or tactics under which it falls is determined. Fourth, a determination is made whether it is a substantially new technique or whether it is already documented in ATT&CK. Here, one of three possible approaches can be taken: (a) adding an entirely new 5G Technique; (b) adding a new 5G sub-technique under an existing technique, and (c) extending an existing ATT&CK technique or sub-technique to cover 5G - these are called "addendums". To arrive at a decision in this step, consideration is given to various aspects, with the most crucial being whether or not the 5G technology, architecture, or design drive fundamentally different adversary behaviors than the counterparts of Enterprise or Mobile matrices. Other aspects are possible mitigations, possible detections, and defender group affinity.

As a final step, the technique is developed with a description and various metadata labels similar to those in ATT&CK: architecture segment/platform, assets, detections, mitigations, references, pre-conditions and post-conditions. After this, the technique is ready to incorporate into the FiGHT matrix. FiGHT is compatible with ATT&CK but it is a separate framework that includes theoretical threats.

It is worth noting that this process is not an exact science, but rather a subjective art, which is subject to change during the maturation process of the framework. Threat modeling is also an iterative process, where additional, regular releases are needed to keep up with advances in adversary behavior, new observations by defenders of adversary behavior, and feedback from those who will use the threat model.

IV. 5G System Model

There are several dimensions or views of the 5G system, as shown in Fig. 2. The reason for the development of each of these views is twofold: to help categorize threats in such a way that enables operationalization of the threat framework, and to ensure all areas are covered in terms of potential threats.

A. The Architectural components View

A 5G system consists of several architectural elements. At the wireless edge of the network there are User Equipment (UE), which is the device (smartphone, smart sensor, vehicle); Radio Access Network (RAN), which can be disaggregated as in the OpenRAN architecture, with Radio Units (antennas mounted on poles for examples) communicating via fiber cables with the more centralized components of the base station, namely Distributed Units (DUs) and Central Units (CUs); and Multi-Access Edge Computing (MEC) components. Non-3GPP access (e.g. WiFi as it is used to access the core network) also fits here.

The Core Network (CN) encompasses network functions (NFs) that support user and business use cases; they communicate via either Service Base Interfaces (SBI) or Non-SBI—meaning other paradigms of communication.

Network Slices are a special element because it is a logical grouping of components that can span from RAN to CN, with many combinations of shared vs. dedicated functions.

At the edge of the 5G network there are the data networks, and the functions that support Roaming, interconnect, IP Multimedia Subsystem (IMS) and interworking between operators' networks).

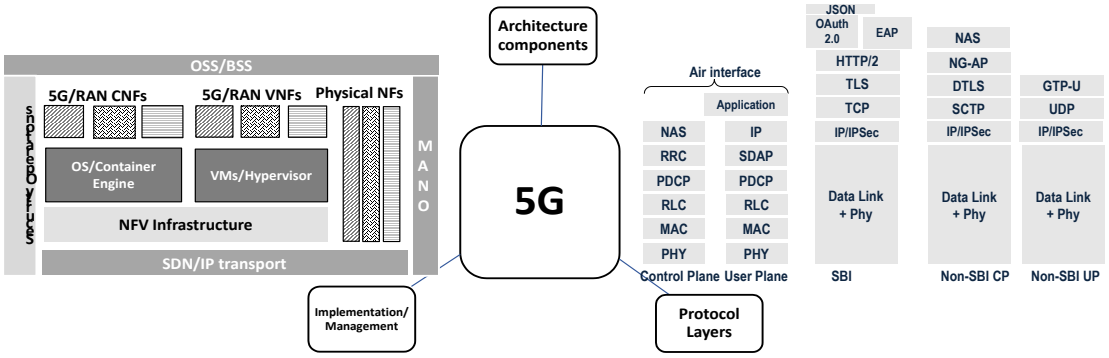

Fig. 2 Dimensions of the 5G system

B. Implementation/Management View

A typical deployment of a 5G system can in principle use traditional hardware and software components such as base stations (gNBs), network functions, databases, and communication links. However the trend is for "Softwarization" of the telecommunication infrastructure due to the flexibility that it provides in how networks are composed, enabling service level agreements (SLAs) to be delivered on. Hence, we show the several options for cloud-based deployments: at the top there are Operations Systems Support (OSS) and Business Systems Support (BSS). Below are RAN nodes and NFs deployed in containers or virtual machines (VMs); these use software defined networking (SDN), which typically runs on generic compute infrastructure, networking, and data storage components. Across all these layers is a management and orchestration (MANO) function that separately manages each of these components (e.g., the infrastructure vs. the containers). Supply chain (not shown in picture) also fits in this view. All of these components come with their own threats.

C. Protocol Layers View

This view is arguably the oldest as it has been used since 2G. 3GPP defines "stacks" or protocol layers that depend on the communication endpoints. These layers loosely follow the OSI layers, but 5G protocols are transport specific and thus often reuse the upper layers (IP, TCP). In other words, 3GPP either reuses "as is" upper layers protocols (e.g., TLS (Transport Layer Security), HTTP/2 (Hypertext Transfer Protocol/2)), or it defines their use for purposes of 5G (e.g. REST APIs (Representational State Transfer Application Programming Interface), TLS profiles). The types of communication links can be broadly categorized as follows: (a) Air interface (UE to Radio Access Network communication, which has a control plane and a user plane components); (b) Service-Based Interface (SBI) (signaling between Network Functions within the operator network), (c) non-SBI control plane (end to end UE to core network function signaling), and (d) non-SBI user plane (end to end UE to data network subscriber/user traffic).

We note that each type of communication link is protected with different security mechanisms, chosen to suit the risks – such as ease of access – associated with that interface.

V. Security Sub-domains of 5G for Threat Modeling

There are several security domains within a 5G system. Each security domain encompasses two or more type of nodes communicating data, which can be user plane (e.g., subscriber's applications like content streaming), or control plane (i.e., the signaling that the network functions exchange to support the data services of a user). What distinguishes them is the accessibility (from an adversary perspective) to the components, and the specified security controls on the communication interfaces. This in turn affects the type of threats that can be encountered. Our approach of breaking down security (trust) domains for purpose of threat modeling is as follows:

A. Radio Interface

In this sub-domain, user devices communicate with the radio access network nodes (gNBs, nG-eNBs, WiFi access points). This segment has seen a lot of attention in 5G, as it is traditionally viewed as the most exposed and critical to secure (i.e., restrict and control access to) to protect the operator's business. With 5G, there is mandated[1] integrity protection, not just confidentiality protection like in previous generations, for user data. The algorithms for these use symmetric keys and are the same as for 4G; they were chosen for adequate security and bandwidth efficiency, given the relatively constrained air interface. Thus this security sub-domain has high accessibility

[1] Such mandates by specifications can be preempted by local regulations.

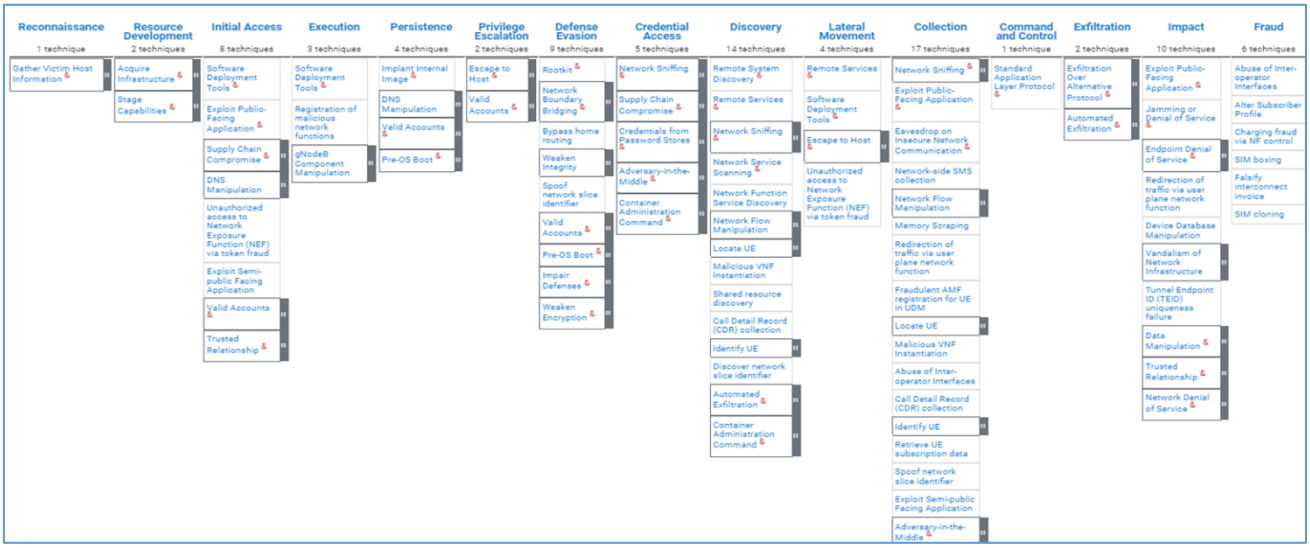

Fig 3. FiGHT framework website.

but is deemed to be protected at an adequate level (according to specifications).

B. Non-SBI (Non Service Based Interface)

This sub-domain connects the radio access network to the core network. It is less exposed to adversaries than the air interface but also potentially more exposed than the core network. The specifications call for "Network domain security", meaning IPSec or physical security. It is worth noting that the cost of protecting these links (in terms of bandwidth) can be deemed high by a given operator and in practice IPSec tunnels may not actually be activated on such links.

C. SBI (Service Based Interface)

This sub-domain connects the core network functions via limited/strictly specified messaging in the style of consumer-producer. The links are specified to be protected via TLS and using a prescribed set of REST APIs. To avoid the many-to-many links, it is possible to deploy a service-based proxy. At the edge of such a network domain there are firewalls or other functions restricting access to the rest of the network function, such as the Security Edge Protection Proxy (SEPP) and Network Exposure Function (NEF). Thus, accessibility to this domain is viewed as hardest to achieve compared to the other domains. The TLS links set up via digital certificates for both parties are in place to afford the highest level of security chosen from the arsenal of commercial systems.

D. Roaming/Interconnect

This sub-domain is neither public facing nor internal, but rather "semi-public", i.e. access is restricted to operator's SEPPs, IP Exchange (IPX) providers, and other authorized roaming/interconnect servers or user plane functions (UPFs). This domain also received special attention in 5G due to the breaches / abuse incidents that operators have experienced. To address these issues, the SEPP was introduced, but the fact that many operators do not have 5G networks yet means that interconnect with lower generations networks is still supported. The type of protection between the 5G SEPP is either TLS based or JavaScript Object Notation (JSON) Web Encryption (JWE) and JSON Web Signatures (JWS) based. Accessibility to this domain is somewhere in between that of the core network and the radio interface, and its security controls can be assessed similarly to those counterparts used in the Internet today.

When studying a complex system like 5G from a threat perspective, one should strive to achieve the right level of abstraction, and this starts with the sub-domains. One very high level of abstraction could be to view the system as having only two components; the radio interface that UEs use to connect, and the rest of the network. Another view takes the lowest level of abstraction, down to the communication protocols protection details, under each of the four domains above. For example, the roaming/interconnect can carry user traffic (UPF to UPF), or signaling traffic between SEPPs; this signaling traffic in turn can be either control messages ("N32-c" interface) between SEPPs or "forwarding" messages ("N32-f" interface) between NFs in the two networks, going via the SEPPs. For FiGHT, we chose a mid-level of abstraction whereby we distinguish threats based simply on the four sub-domains outlined above.

E. Example of Threat Coverage Analysis per Sub-domain

Reviewing, evaluating, and decomposing by sub-domain known and hypothesized threats is a useful exercise that can identify gaps in current coverage. This process can also ensure a more complete coverage of the actual or potential adversarial techniques throughout the 5G system. For this example, we choose the following three techniques: Adversary in the Middle (AitM), Network Sniffing, and Data Manipulation. AitM is a method where an adversary acquires a position between two entities interfacing across a network (interface or end node), and paves the way for the other two techniques: Network Sniffing, which tries to take advantage of weakly encrypted or unencrypted transmissions (i.e., gathering user or signaling traffic), and Data Manipulation (i.e., injecting spoofed messages or changing data packets in transit). A similar approach is used to analyze other popular techniques like Denial of Service (DOS).

Enterprise counterpart and tools or procedures are needed to achieve this goal. The goal is to decide for each technique how it applies to each of these domains. To this end we assess a) whether the adversary behavior is substantially different from its Enterprise counterpart (qualitative difference ranked High, Medium or Low) and b) tools or procedures needed to achieve this goal. We note that the assessment of a) is subjective, while b) may contain only a representative example. The results are presented in Table I.

TABLE I. EXAMPLE OF ADVERSARY SKILL LEVEL AND TOOLS FOR EACH DOMAIN INFLUENCE TECHNIQUE GROUPING TYPE STYLES

	Security sub-domain	Radio Interface	Non-SBI	SBI	Roaming/interconnect
Adversary in the Middle	Qual. Difference /tools	High / Fake base station	High / UPF or router compromise	High/ Core NF compromise	High/ Proxy compromise
	Threat curating verdict	*Separate subtechnique*	*Separate subtechnique*	*Separate subtechnique*	*Separate subtechnique*
Network Sniffing	Qual. Difference / tools	Medium /Wireless receiver	Low / IP packet capture	Low / IP packet capture	Low / IP packet capture
	Threat curating verdict	*Separate addendum*	*Same addendum*		
Data Manipulation	Qual. Difference / tools	High/ Fake device+ base station	Medium /NF or router compromise	Low / Proxy or NF compromise	Low/router/ or Proxy compromise
	Threat curating verdict	*Separate addendum*	*Same addendum*		

VI. THE FRAMEWORK AND ITS OPERATIONALIZATION

A. The website

The FiGHT framework is available as a website [9], and a screen capture of it is shown in Fig. 3. The website can be "navigated", and each of the tiles contains one technique, which may have one or more sub-techniques that can be expanded under it (this is signaled by the dark right side of the tile). A new webpage is displayed when clicking on a given tile, which, as shown in section III, contains more information for that threat.

It is informative to give a few examples of some new 5G FiGHT techniques, sub-techniques or addendums to existing ATT&CK entries. Examples are given by security sub-domain.

Example of new tactic: Fraud. It is defined as "The adversary is trying to obtain service without contractually paying for it".

Examples of new 5G techniques/sub-techniques, for two architectural subdomains:
Core network SBI: A new 5G technique is "Registration of malicious NF", under the tactic "Execution". It was deemed that no existing ATT&CK technique covers this adversarial behavior. The description is "An adversary, such as an insider to the MNO or vendor, could install a malicious NF into the core network, in order to launch other attacks or get access to information." In 5G, each new instance of a NF (e.g., a new Session Management Function (SMF) must register itself into the Network Repository Function (NRF), before it can participate in the core network signaling. Especially in cloud environments, it is plausible that an adversary registers a new NF instance in the NRF, as an insider or after penetrating the operator's network.

Radio Interface and SBI: A new 5G technique is "Identify UE", under the tactic "credential access". The description is "Adversary may obtain UE permanent identifier via various means". The permanent identifier of a UE is an important 5G asset because it opens to the door to mount other attacks against this UE. In 5G, the UE identity International Mobile Subscriber Identity (IMSI) was replaced by the Subscriber Permanent Identifier (SUPI), which can be concealed by the Subscriber Concealed Identifier (SUCI). This new technique has three sub-techniques: 1) intercept home network via SUCI, 2) intercept IMSI via bid-down UE, and 3) obtain SUPI via NF signaling. The first two sub-techniques belong to the Radio Interface sub-domain and the third to the SBI sub-domain.

An example of a new 5G sub-technique under an existing TT&CK technique is:
Core network Non-SBI: Under the ATT&CK technique "Adversary in the Middle" (AitM) (T1557), a new 5G sub-technique called "Non-SBI" is added, with description: "Adversary with access to Non-SBI network nodes may position themselves in order to eavesdrop or manipulate user plane and control plane traffic". This is being added because none of the sub-techniques to the Enterprise AitM, nor the Mobile AitM (T1638) cover this 5G specific method.

An example of a 5G addendum to an existing ATT&CK (sub) technique is:
Radio interface: The ATT&CK sub-technique "Endpoint Denial of Service: Service Exhaustion Flood" (T1499.002) can have a 5G context: An addendum called "Base Station flood with fictitious access requests" covers this adversarial behavior of sending a large number of access requests over Random Access CHannel (RACH) to degrade the ability of legitimate UE to obtain access from the gNB.

B. Lessons learned from applying threat curating methodology to 5G

The following observations are made in this process. The language use differences between telecommunications and enterprise networks made this technique development somewhat challenging. Sometimes new terms were introduced-for example, "semi-public", to distinguish network functions that are not public-facing, nor operator-internal. Generally, the tactics remain mostly unchanged. Adversarial goals are still the same, at a high level, as the ones experienced in attacks to the enterprise system. There was only one tactic deemed to be

sufficiently distinct to be added, namely fraud. A type of impact, fraud has been at the forefront of mobile operator's security concerns since early generations. As for the definition text of the tactics, we found that they are largely applicable as stated to the 5G environment. In only one case the description falls short, namely "credential access", and this is due to the simple fact that in 5G, there are other credentials used besides passwords.

C. Operationalization of FiGHT

To assist with the operationalization of FiGHT, the theoretical threats would have be tested. Just like ATT&CK, FiGHT is a framework to enable the following cybersecurity activities: Adversary emulation, red teaming, behavioral analytics development, defensive gap assessment, Network and Security Operations Center (NOC/SOC) maturity assessment, Cyber Threat Intelligence (CTI) enrichment, etc. Expanding on some elements of this list, the FiGHT framework can be used to support such goals as:

Build asset focused attack trees. Each technique and sub-technique have one or more assets that the adversary is targeting. This aids the buildup of asset focused attack trees: e.g., if the asset is user location, an attack tree shows possible paths to find a user's current location, given their phone number.

Emulate Adversaries: Adversary emulation can be done manually, which is error-prone and time consuming. Autonomous adversarial emulation tools exist, for example CALDERA which is mapped to the MITRE ATT&CK framework. Such tools would have to be extended to cover 5G and be mapped to the FiGHT framework.

Get a comprehensive view of all threats to a particular 5G architectural segment. In cases where, for example, threats to the inter-operator roaming interconnect fabric are of concern, the matrix can be reduced to show only threats that affect the roaming/interconnect network functions and communication links. This may be desired in cases where the operator experiences increased breach attempts via the interconnect networks. An example of such is a warfare-related attack that relied on the roaming communications, described in [10].

Share threat intelligence. Threat data can be formatted using the STIX™/TAXII (Structured Threat Information Expression, Trusted Automated eXchange of Intelligence Information), to allow the automatic exchange of threat information between IT security and threat intelligence systems of various organizations. Given the increase in types of stakeholders that 5G brings – such as cloud providers – it is expected that such tools will be well employed in the goal of securing 5G networks at all levels.

Planning Cyber investments. Tactics and techniques can be used to assist architect and program managers to plan, acquire and deploy needed security controls for their enterprise systems when utilizing 5G as part for their solutions.

Risk-driven prioritization. Military environments tend to adjust to risk posed to assets. A 5G Tactical solution may require different risk mitigation techniques when deployed on a CONUS base compared to when used in NON-US theater.

Security Maturity and Posture Assessments. FiGHT can be used to assess organization's risk posture and their ability to enhance their protect, detect and respond capabilities.

VII. Conclusions

There is a growing need to address the security of the 5G networks via an overarching threat framework. This paper introduced FiGHT, a knowledgebase of observed and hypothesized threats against a 5G system. The FiGHT framework covers all sub-system aspects of 5G. We describe the process of curating threats from various sources, provide a breakdown of the 5G system into architectural components that share similar security posture, and give an example of how threat coverage across these domains was achieved. We conclude by showing how this 5G threat knowledgebase can be operationalized to secure various deployments.

Acknowledgment

We are grateful for the helpful comments received from the team of subject matter experts in MITRE. The FiGHT project would not have been possible without the outstanding contribution of Muddasar Ahmed, Eric Arnoth, Tom Bibbo, Surajit Dey, Andrew Foote, Kevin Mauck, Andy Pyles, Andy Radle, Michael Recchia, Ben Schmidt, Amir Stephenson.

References

[1] MITRE, "MITRE ATT&CK," MITRE, 2022. Retrieved at https://attack.mitre.org.

[2] European Union Agency for Cybersecurity (ENISA): "ENISA Threat Landscape for 5G Networks" Report, December 2020. Retrieved at https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

[3] S.P. Rao, S. Holtmanns, T. Aura: "Threat modeling framework for mobile communication systems", May 2020. Retrieved at https://arxiv.org/abs/2005.05110v1

[4] R. Pell, S. Moschoyiannis, E. Panaousis, R. Heartfield, "Towards dynamic threat modelling in 5G core networks based on MITRE ATT&CK", October 2021. Retrieved at https://arxiv.org/abs/2108.11206

[5] GSM Association, "5G Cybersecurity Knowledge Base," GSMA, 2021. [Online]. Available: https://www.gsma.com/security/5g-cybersecurity-knowledge-base/. [Accessed May 2022].

[6] Third Generation Partnerhip Project (3GPP), TR33.926, "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes", Technical Report, v17.0.0, 2021

[7] Third Generation Partnerhip Project (3GPP), TR33.848, "Study on Security impacts of Virtualization", Technical Report, v0.14.0, 2022

[8] Ericsson blog, "Cyber Threat Intelligence: Understanding attack patterns in mobile networks". Retrieved at https://www.ericsson.com/en/blog/2022/6/cyber-threat-intelligence-mobile-networks.

[9] https://fight.mitre.org

[10] Cathal McDaid, "The hunt for HiddenArt", blog article , February 2022. Retrieved at https://blog.adaptivemobile.com/the-hunt-for-hiddenart