A. Nieto, “An Overview of Proactive Forensic Solutions and its Applicability to 5G”, *IEEE 5G World Forum (5GWF)*, pp. 191-196, 2018.
http://doi.org/10.1109/5GWF.2018.8516940
NICS Lab. Publications: https://www.nics.uma.es/publications

An Overview of Proactive Forensic Solutions and its Applicability to 5G

Ana Nieto
Network, Information and
Computer Security (NICS) Lab
University of Malaga (Spain)
Email: nieto@lcc.uma.es

***Abstract*—This article analyses the state of the art of proactive forensic solutions and highlights the importance of preparing the 5G ecosystem to serve digital forensic purposes. The analysis considers the current 5G threat landscape from the ENISA report, and discusses how some of the attacks could be mitigated using proactive forensic mechanisms. In addition, the requirements for deploying proactive forensic solutions in 5G are classified, and analysed based on the specific threats against 5G.**

I. Introduction

Proactive digital forensics (onwards proactive forensics) is a relatively new term that has not yet been applied to 5G environments. Unlike traditional digital forensics, proactive approaches are more dynamic, enabling the system to collect digital evidence periodically, without stopping the functioning of the IT infrastructure (in optimal cases, c.f. Section III). Although not all systems support this type of action, proactive digital forensic solutions for 5G would allow them to slow down attacks if these are combined with known network security elements (e.g. IDS, SIEMs).

The main objective of this paper is to analyse current proactive forensic approaches to extract a set of requirements to enable their application in 5G environments. As discussed at the end of the paper, the requirements to deploy proactive forensic approaches in 5G could introduce some risks into the infrastructure if security mechanisms are not properly ensured. To analyse these issues, the taxonomy of SDN/5G threats (ENISA report [1]) is taken as the basic model of reference during the analysis.

The structure of the paper is as follows. Section II provides a basic review of the ENISA threat landscape for 5G, focusing on those aspects that are relevant to the contribution of this paper. Section III provides initial assumptions and defines the requirements to design proactive digital forensic solutions in 5G. The list of requirements for the applicability of proactive forensics in 5G are identified, based on the analysis of the proactive forensic solutions provided in Section IV. Section V discusses how the proactive forensic requirements can affect security in 5G environments. Finally, Section VI summarises the conclusions of the paper.

II. Background - SDN/5G Threats

The ENISA threat landscape presented in [1] has two distinct parts: i) general categories of threats which are inherited from a previous, general report, and ii) the classification of threats depending on their source: SDN element, 5G element or generic network element. Fig.1 provides a graph with the information about threats in [1] considering the second classification, which is more specific and relative to this article.

Note that, because a 5G system combines the SDN architecture with the virtualisation of the network functions (as well as other virtual components) and the radio access technologies (RAT) for 5G, we can see that the threats of group B - right of Fig.1 - can be included in group A - left of Fig.1. This analysis considers this fact focusing on the slope of attacks that could affect several layers, denoted as cross-layer attacks.

The group of threats in A define the specific threats to SDN considering the division in the three layers of an SDN architecture [2]: data or infrastructure layer (network devices), control layer (SDN control software) and application layer (e.g. business applications). The analysis in this paper considers this structure, but also includes the *end-user* layer as one additional layer needed to classify the proactive forensic requirements for 5G (c.f. Fig.2). Furthermore, it is important to clarify, that in [1] a list of tools to mitigate the threats is provided and analysed. Although the information provided by these tools is very interesting from a digital forensic perspective, the focus of the report is quite different and does not consider an integration of these tools with proactive forensic solutions, which is extremely useful to help understand and analyse the nature of the most sophisticated attacks.

In addition, proactive forencics can be particularly helpful to understand the context of a cross-layer attack. Cross-layer attacks affect the different layers of a system or architecture, that can be subject to different requirements - or under the control of external entities - and therefore, are very difficult to track and follow. The problem is further complicated when several infrastructures are affected.

In [3] a taxonomy of attacks on the 3G Network is presented. The authors differentiate between Cross Infrastructure Cyber attacks and Single Infrastructure attacks. The first are motivated by the Internet connectivity to 3G networks and the nature of the *Cross Network Services* (CNS) which combine Internet-based data and data from the wireless telecommunication network to provide services. Three examples of CNS are provided - Email Based Call Forwarding Service (CFS), Client Billing Service (CBS) and Location Based Instant Mes-

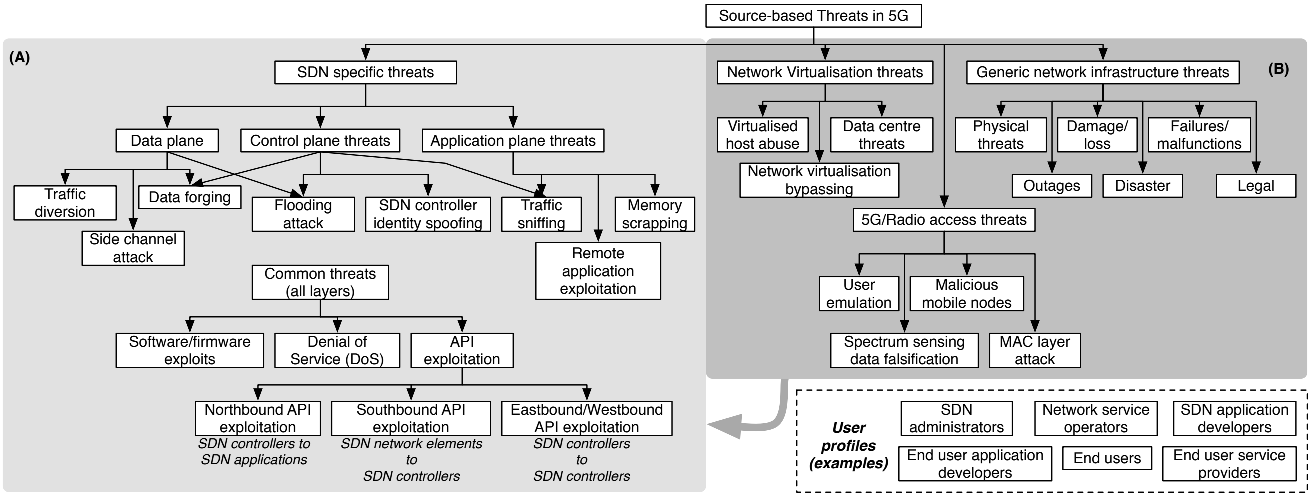
Source-based Threats in 5G
(A)
SDN specific threats
Data plane
Control plane threats
Application plane threats
Traffic diversion
Data forging
Flooding attack
SDN controller identity spoofing
Traffic sniffing
Memory scrapping
Side channel attack
Remote application exploitation
Common threats (all layers)
Software/firmware exploits
Denial of Service (DoS)
API exploitation
Northbound API exploitation
SDN controllers to SDN applications
Southbound API exploitation
SDN network elements to SDN controllers
Eastbound/Westbound API exploitation
SDN controllers to SDN controllers
Network Virtualisation threats
Generic network infrastructure threats
(B)
Virtualised host abuse
Data centre threats
Network virtualisation bypassing
Physical threats
Damage/ loss
Failures/ malfunctions
Outages
Disaster
Legal
5G/Radio access threats
User emulation
Malicious mobile nodes
Spectrum sensing data falsification
MAC layer attack
User profiles (examples)
SDN administrators
Network service operators
SDN application developers
End user application developers
End users
End user service providers

Fig. 1. Summary of 5G specific threats from the ENISA report

saging System (LB-IM). Additional examples are provided in [4]. Cross-infrastructure attacks are possible, given that there are attacks which affect the Internet and are propagated to cellular networks. It is unrealistic to assume that the security improvements in 5G will be sufficient to ensure that these types of attacks will no longer be possible.

An additional issue is the false sense of security that some technologies may bring about. For example, 5G relies on the use of advanced virtualisation technologies (e.g. NFV), and one of the security measures of these is precisely the isolation that such technologies offer. However, several papers have proven that security containers can be broken (indeed, this is one of the threats in Fig.1, group B). In [5] a cache-based side-channel attack on AES is demonstrated. The attack enables a full key recovery across a virtual machine in a cloud-like server setting. The attack exploits the memory deduplication feature which is intended to enable resource sharing to increase the performance of the platform. Similarly, there are diverse attacks on known implementations of SDN, some of which are described in [6], [7]. Furthermore, a major concern are those attacks whose main objective remains undiscovered until it is too late to stop them or to save any piece of evidence to discover the perpertrators or help prosecution of the cyber-criminal. If the attacks use non-affected devices that act only as intermediaries between the infrastructure and the attacker, and do not affect the performance or the QoS of the infrastructure until it is too late to be stopped, then it will be extremely difficult to collect digital evidence based on pre-defined rules.

Therefore, proactive forensics will not only be critical to understand the nature of the cyberattack, but also to stop or to mitigate its effect.

III. Requirements to design proactive digital forensic solutions in 5G

In [8] a proactive architecture for database forensics is provided considering *Chain of Custody* (CoC) restrictions by design. As the authors state, the need for proactive forensics is clear; unlike *reactive forensics* which is devised to send an alert if some preconditions are true, *proactive forensics* is conceived to prepare the system to collect digital evidence to be analysed by experts in the field. Therefore, while the first *react* against something known, a *proactive* system will not only react, but also should store the information following certain procedures accepted by the forensic community - for example, to maintain a chain of custody. This also simplifies the analysis of large sets of data, because these are stored taking into account the usual requirements for analysis by experts (e.g. key fields, relationships between user entries).

Another approach is to consider that reactive forensics is the traditional approach for digital forensics, while proactive forensics is the use of real-time forensic technologies or live forensics [9], to acquire digital evidence as quickly as possible (e.g. for memory analysis), and in some cases without interrupting the working devices in the network (e.g. requirement in industrial networks). Note that, to be effective, the network should be prepared for forensic analysis. However, unlike the first approach, this does not require that the devices, network components, or more generally, the sources of information, are able to provide the information in a specific format with the specific requirements pursued by the forensic analysis.

In [10] the authors differentiate between a) proactive *"before an incident alert or evidence request"*, b) active *"during a live or real-time incident"*, and c) reactive - *"after an incident"*. In the rest of the paper a) and b) are grouped in the term proactive.

In this paper the previous approaches are considered in a combined fashion. Our understanding is that, a proactive forensic approach for 5G environments should satisfy both premises as basic requirements: (i) some or all the components in the system are prepared to take proactive actions following a set of rules to maintain the integrity of the CoC for the admissibility of the digital evidence and (ii) the tools used to interact with

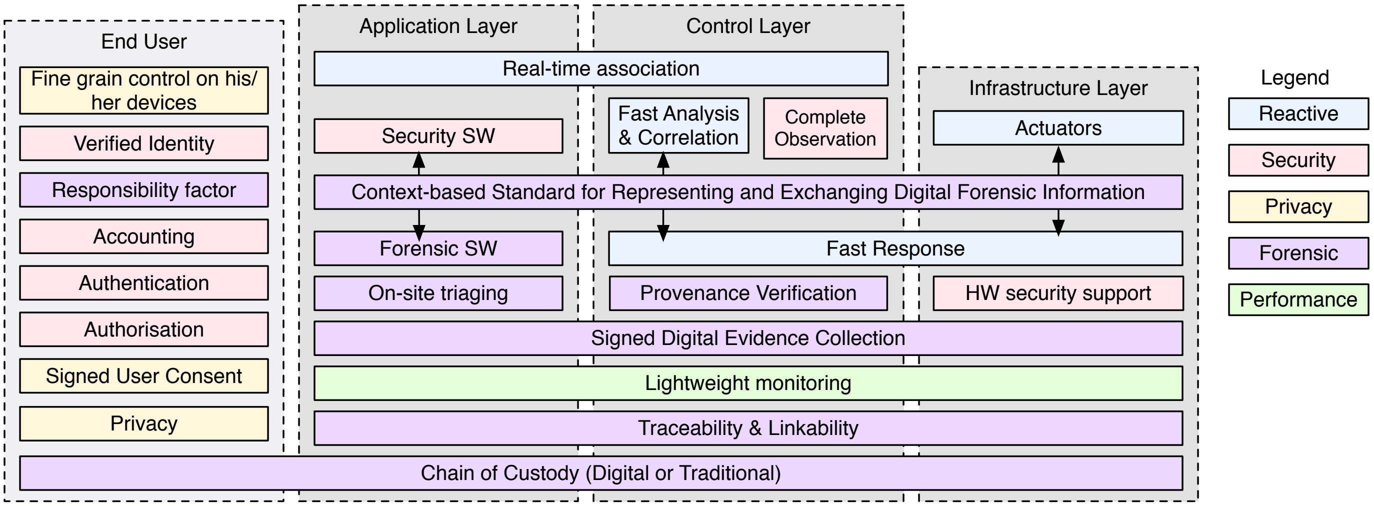

Fig. 2. Requirements for Proactive Digital Forensics in 5G

the elements to be analysed respect the functionality, the nature or limitations (e.g. resource-constrained) and the performance (e.g. the main task to be done by the element in the network) of the system.

Following these premises, Fig. 2 shows the basic set of requirements identified for proactive forensics in 5G environments that are considered in this paper. The requirements have been identified based on the analysis of the solutions for proactive forensics proposed in the literature (Section IV). In addition, the requirements are classified based on the definition of the layers of a typical SDN architecture topology [2], [1] (c.f. Section II): application, control and infrastructure. Therefore, this simplifies the mapping with the 5G threat landscape in [1] (c.f. Section II).

Note that, in this approach, an additional layer is included, the end user layer, considering the human assets in [1], from which different user profiles can be identified (c.f. Fig.1). This new layer is only considered to complete the classification of requirements for proactive forensics in 5G with the requirements that will affect a person. It is important to highlight that a traditional CoC is highly dependent on the individuals who have access to the digital evidence.

In addition, one of the objectives of this article is to identify if the solutions to support these requirements can be applied end-to-end. It is also important to analyse whether the proactive forensic tools applied in different, separate layers could be used to understand the whole context of a cyberattack. Intuitively, all the components, entities and actors in the 5G environment have to be carefully considered together in order to understand the whole context for a forensic investigation. However, narrowing the forensic investigation as much as possible - when it is possible - is also important for performance, scalability and data minimization.

IV. Proactive Digital Forensic Solutions

As stated in [9], the allusion to *proactive forensics* in the literature comes in two forms: explicit and implicit. The following analysis of proactive forensic solutions is conducted considering both, paying particular attention to its applicability to 5G ecosystems.

A. *End users, applications and devices*

Some possible approaches to applying proactive forensic approaches in personal devices have been proposed in [11] and [12]. In [11] a Proactive Smartphone Forensic Scheme is proposed. The solution collects the digital evidence from the mobile phone using a software agent, the evidence is stored in a database towards an independent authority that has the role of trusted third party between the device and the investigator. In [12] personal devices with embedded security features are used to collect digital evidence. One of the limitations of the current computer forensic solutions for personal devices is the lack of standards which consider these devices as cooperators in forensic investigations, and therefore the lack of common formats to be used for the proactive collection of digital evidences. In [10] a solution denoted ProDF (Pro-active Digital Forensic) is proposed to help an organisation to implement proactive forensics in accordance with good practices. ProDF considers the internal organisation of a company (e.g. policy, people, technology) and could help to determine the dimension of the incident. This kind of framework could be very helpful in a company, but cannot be directly applied to multi-tenant architectures or to personal devices not under the control of the company. In [13] a high-level architecture for collecting secure digital evidence - defining a *Digital Chain of Evidence* (DCoE) - from different actors in the environment (application servers, network level actors such as intrusion detection systems or sensors for physical events) is presented. The architecture relies on an interactive explorer of a forensic data-base, so this solution could be considered a proactive but not a real-time solution, because the digital chain of evidence is not necessarily created at run-time. The system is based on the use of trusted computing hardware to control secure evidence generation. A critical issue is the requirement for real-time association, which is related to the capacity to establish a time line for the digital evidence collected. Note that this requirement affects the application layer when the digital evidence is pre-processed, in local, in the device before being sent to other entities in the chain, and also to the control layer if the time-line is established just by the components in the control layer (e.g. a virtual service).

Additional solutions relying on software agents but not prepared (yet) for heterogeneous, resource-constrained devices are *Google Rapid Response* (GRR), Facebook osquery or *Mozilla InvestiGator* (MIG). These solutions, classified as Remote Live Forensics solutions, denote a clear tendency to deploy proactive forensic solutions to help to protect to clients and end-users of the network in a controlled environment. Similarly, in [14] a *Proactive Process Monitor* (PPM) is proposed for insider threat detection and proactive forensics. The solution decomposes the problem in three detection levels: known malicious or unauthorised processes, pre-defined rules for detection, and anomalous behaviour. The approach concentrates on how IDSs can be used to collect digital evidence, but does not consider critical digital forensic requirements such as the legal compliance of the digital evidence or the admissibility.

Finally, there are some contributions that could be useful to understand the nature of digital forensic principles applied to cellular networks but that cannot be considered as proactive forensics. For example, in [15] a guideline on mobile device forensics is provided. The document details the procedures for the collection and analysis of physical evidence following the traditional approach and the use of tools to acquire the digital evidence from the sources. The mobile device tool classification system is based on a set of levels: manual extraction, logical extraction, hex dumping/JTAG, chip-off and micro-read. The results of this analysis provide a rich classification of tools for acquiring digital evidence from cellular networks - type GSM, CDMA and iDEN/TDMA. However, considering the requirement of non-interruption requested in Section IV, the tools provided in the report cannot be considered proactive.

It must be stressed that one of the key challenges will be to apply *isolation* techniques to ensure that data extraction is not affected by external entities (e.g. Cellular Network Isolation Card (CNIC) feature). In addition, the case of an on-site triaging process is useful when we consider a preliminary analysis of the data extracted can be required at the scene. This is is still a reactive approach (c.f. Section III).

B. Control and orchestration of network elements and services

SDN and NFV are two key technologies that will be used in the control layer, for the orchestration of services in 5G. In this context, there are two types of approaches: i) how these new technologies can be problematic in digital forensics (e.g. lack of a regulation, the location of the resources is not always known, loss of digital evidence due to the re-configuration, migration, etc.), and ii) how these technologies can be used to improve the digital forensic investigation in a system with these technologies (e.g. to use the fact that SDN controllers are intermediaries). Regarding the first point, in [16] specific problems to carry on digital investigations in virtual networks are analysed. In [17] two main problems in virtual networks are highlighted: migration and customisation. Both affect traceability and loss of information. In addition, in [18] it is demonstrated that abstract layers typically used in a virtual environment (e.g. virtual memory abstraction) can affect the collection of digital evidence. Some approaches that deal with these issues are described below.

In [17] the tool ForCon implements a virtual network forensic framework to collect digital evidence using SDN agents. Some requirements to extract digital evidence using SDN can be extracted from [19], where SDN middleboxes, denoted as PVP (*Provenance Verification Points*) are used to collect forensic information from data centers. One interesting feature is the *lightweight monitoring*, to ensure that the PVPs will not be slower than the network's real time communications, to ensure the *complete observation* property.

However, the volume of data and the heterogeneity of the sources can become a bottleneck for real-time analysis in 5G. To prevent this, the use of common formats for digital evidence is recommendable. Moreover, in large-scale systems, cooperation and information sharing are mandatory to promptly detect attacks against the users or the infrastructure and for mitigation. In [20] a comparison between schemas for digital forensic information is provided, and an ontology is proposed to standarise the representation and exchange of digital forensic information (DFAX, *Digital Forensic Analysis eXpression*). The ontology considers different parameters (e.g. victim's action) that are finally linked to external concepts such as identity, *Trusted Third Party* (TTP) and observability.

It is important to remark that a common language to express digital forensic capabilities is fundamental to delimit and reduce the set of digital evidence. This can be based on criteria such as the origin of the data, the robustness of the collector or other criteria that could be more subjective to the investigator in charge (e.g., trust in a system given its reputation). Moreover, a common language framework is also critical to help investigators in different jurisdictions to identify similarities between attacks in order to prosecute the cybercriminal. A critical point is that digital forensic investigators must be able to differentiate between different domain layers which is also required in 5G, given its complexity.

Additional important requirements highlighted in [13] (c.f. Section IV-A), where the digital evidence collected from different components in the network (e.g. IDS, sensors, firewalls) are processed in a centralised entity, are scalability and the need to support the exploration of large graphs with semantically enriched information. These requirements are closely related to the fast analysis and correlation requirement, and the need to define specific common formats to share relevant information between the components of the proactive forensic system. To increase the performance in forensic analysis the approach in [22] suggests providing digital forensics as a service. This is closely related to the approach in [19] (how SDN could help a digital forensic investigation). In other

TABLE I
PROACTIVE FORENSIC SOLUTIONS

Solution	Final user	Sources	Collector	TTP	Restrictions	Proactive
PSFS [11]	Investigator	Mobile phone (suspect)	Software agent in the source	TTP between final-user and Source	External data base	Explicit
Digital Witness [12]	Citizen, Investigator	IoT devices with security capabilities	Software agent in the source & Authorised Points	Distributed - embedded in the device	HW security support (TPM,SE)	Implicit
ProDF [10]	Company	IT Infrastructure	IDS	No	High level policies	Explicit
HL architecture for DCoE [13]	Investigator	IT infrastructure	Interactive explorer for forensic DB	TPM in source	HW security support (TPM)	Explicit
PPM [14]	Administrator	Network elements	IDS	No	IDS-based approach	Explicit
ForCon [17]	Investigator	Data plane network elements	SDN agent	No	SDN architecture	Implicit
PVP-based [19]	Administrator	Data plane network elements	PVP (SDN middleboxes)	No	SDN architecture	Implicit
WEVAN [21]	Offender vehicle	surrounding vehicles	Source & Counter evidence analyser	Certification authority	VANET	Implicit

words, the combination of services for digital forensics plus the versatility and dynamic nature of SDN could help provide natural solutions to deploy digital forensic solutions in 5G.

C. *Proactive solutions directed to 5G use-cases*

An interesting characteristic in 5G is network slicing. This feature enables the separation of the final use cases in a 5G environment in different layers, by separating the flows, and, therefore, enabling the configuration of specific services per use case. This could help define specific procedures for digital evidence collection in a complex environment such as 5G, if the security of the process to do that and the integrity of the data collected can be ensured. The most well-known use cases in 5G are: autonomous vehicle control, factory cell automation (industry IoT 4.0), remote surgery and examination among others [2]. As the previous sections have covered some of these use cases, here the specific use case of vehicular forensics is discussed.

There are recent contributions in the field of digital forensics in the case of vehicular forensics, as is the case of [23] where the authors prove that it is possible to acquire relevant information from the embedded devices in a modern car. However, the procedures shown are quite far from a proactive forensic approach as defined in Section III. The analysis is reactive, performed once the investigators have access to the car, after the event. One of the requirements to perform this analysis without compromising the evidence is the isolation of the vehicle in a Faraday box. Closer to a collaborative and proactive approach, in [21] a mechanism to collect digital evidence is proposed for *Vehicular Ad-Hoc Networks* (VANETs). The mechanism, named WEVAN, considers the vehicles in a VANET as witnesses to acts committed by other vehicles. The requirements for this approach can considered for this particular use case in 5G networks: correctness, confidentiality, authentic request for testimonies and authentic testimonies.

V. DISCUSSION

This section completes the analysis started in Section IV. Table I shows a summary of the high-level characteristics of the proactive forensic solutions analysed, from which the requirements classified in Fig.2 can be extracted. Considering Fig.1, the following paragraphs are dedicated to analyse whether the requirements can mitigate some of the attacks or if they would otherwise make it difficult to identify them or would place an additional burden on the system.

A. *End user*

The objective of the requirements proposed at this level are intended to i) encourage the user to cooperate and also to ii) protect the infrastructure from abuse or misbehaviour. These requirements, although not all explicitly mentioned, are needed, for example, in the solutions proposed in [11], [12] and [21]. The inclusion of the user as an active collaborator in the proactive forensic process requires additional data provided by different user profiles to be handled efficiently. This implies a considerable increase of traffic that could result in false negatives and positives of the systems of identification of threats. If we assume that DoS are avoided by implementing a proper, scalable, proactive forensic system, the risk of including the end-user devices in a proactive approach is that the attacker could find a hole/vulnerability in the communication protocol used and then exploit it to take the control of SDN controllers. These problems could be avoided forcing the collaborators to provide a set of credentials, or prove identity in those critical cases (e.g. an administrator, or evidence of a felony).

B. *Application layer*

The requirements at this layer should be implemented by the applications in the 5G architecture. These applications are the interface between the end user and the control layer, so they are an important point to collect digital evidence.

A serious concern is the possibility that a silent attacker has remote access to the evidence that is obtained at this level. Furthermore, these applications cannot be considered as trustworthy by default. Note that, installing proactive forensic software by default in 5G elements, opens the door to memory scrapping - *an attacker scans the physical memory of a software component in order to extract sensitive information that he/she is not authorised to have* - if a remote application exploitation is possible.

C. Control layer

As described in the previous section, there are proactive forensic solutions specifically designed for SDN, at the control layer. Two of these solutions are [17] and [19]. Due to the fact that the proactive forensic requirements at this layer include complete observation, an effective attack at this layer provides the attacker with control information about the resources of the infrastructure - applications and devices. For example, if SDN-based proactive forensic solutions are implemented using SDN agents in the software components, the attack could be directed to perform data forging against the controllers - *compromising an SDN element in order to forge network data and launch other attacks*.

D. Infrastructure / Data layer

This layer is formed by the devices of the infrastructure, some of which may belong to end users (e.g. shared sensors). Important requirements are the inclusion of HW security support to acquire the digital evidence. It is important whith this to consider the requirements for deploying a digital chain of custody from the origin of the data [12] [14], and implement countermeasures at hardware layer (e.g. memory isolation). This requirement limits possible solutions as they depend on purpose-specific components.

VI. Conclusion

In this paper an overview of proactive forensic solutions is provided, together with a discussion about its applicability to 5G. The analysis has considered the requirements of proactive forensics in the different layers of the 5G ecosystem and the capacity to provide the required functionality without affecting the security of the infrastructure.

Acknowledgments

This research has been partially supported by the Spanish Ministry of Economy and Competitiveness through the research projects IoTest (TIN2015-72634-EXP /AEI) and SMOG (TIN2016-79095-C2-1-R) and FEDER trhough the project PRECISE (TIN2014-54427-JIN). The author has been financed by INCIBE through the grant program for excellency in advanced cybersecurity research teams.

References

[1] A. Belmonte Martin, L. Marinos, E. Rekleitis, G. Spanoudakis, and N. Petroulakis, "Threat landscape and good practice guide for software defined networks/5g," 2015.

[2] A. Osseiran, J. F. Monserrat, and P. Marsch, *5G mobile and wireless communications technology*. Cambridge University Press, 2016.

[3] K. Kotapati, P. Liu, Y. Sun, and T. LaPorta, "A taxonomy of cyber attacks on 3g networks," *Intelligence and Security Informatics*, pp. 129–138, 2005.

[4] F. Sharevski, "Cyberattack surface of the next-generation mobile networks," *Protecting Mobile Networks and Devices: Challenges and Solutions*, pp. 1–17, 2016.

[5] G. Irazoqui, M. S. Inci, T. Eisenbarth, and B. Sunar, "Wait a minute! a fast, cross-vm attack on aes," in *International Workshop on Recent Advances in Intrusion Detection*. Springer, 2014, pp. 299–319.

[6] S. Sezer, S. Scott-Hayward, P. K. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, "Are we ready for sdn? implementation challenges for software-defined networks," *IEEE Communications Magazine*, vol. 51, no. 7, pp. 36–43, 2013.

[7] 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*. ACM, 2013, pp. 165–166.

[8] D. Flores Armas and A. Jhumka, "Implementing chain of custody requirements in database audit records for forensic purposes," 2017.

[9] S. Alharbi, J. Weber-Jahnke, and I. Traore, "The proactive and reactive digital forensics investigation process: A systematic literature review," in *International Conference on Information Security and Assurance*. Springer, 2011, pp. 87–100.

[10] C. Grobler, C. Louwrens, and S. H. von Solms, "A framework to guide the implementation of proactive digital forensics in organisations," in *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*. IEEE, 2010, pp. 677–682.

[11] A. Mylonas, V. Meletiadis, B. Tsoumas, L. Mitrou, and D. Gritzalis, "Smartphone forensics: A proactive investigation scheme for evidence acquisition," *Information Security and Privacy Research*, pp. 249–260, 2012.

[12] A. Nieto, R. Roman, and J. Lopez, "Digital witness: Safeguarding digital evidence by using secure architectures in personal devices," *IEEE Network*, vol. 30, no. 6, pp. 34–41, 2016.

[13] N. Kuntze and C. Rudolph, "Secure digital chains of evidence," in *Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on*. IEEE, 2011, pp. 1–8.

[14] P. Bradford and N. Hu, "A layered approach to insider threat detection and proactive forensics," in *Proceedings of the Twenty-First Annual Computer Security Applications Conference (Technology Blitz)*, 2005.

[15] R. Ayers, S. Brothers, and W. Jansen, "Guidelines on mobile device forensics (draft)," *NIST Special Publication*, vol. 800, p. 101, 2013.

[16] D. Spiekermann and T. Eggendorfer, "Towards digital investigation in virtual networks: a study of challenges and open problems," in *Availability, Reliability and Security (ARES), 2016 11th International Conference on*. IEEE, 2016, pp. 406–413.

[17] D. Spiekermann, J. Keller, and T. Eggendorfer, "Network forensic investigation in openflow networks with forcon," *Digital Investigation*, vol. 20, pp. S66–S74, 2017.

[18] F. Freiling, T. Glanzmann, and H. P. Reiser, "Characterizing loss of digital evidence due to abstraction layers," *Digital Investigation*, vol. 20, pp. S107–S115, 2017.

[19] A. Bates, K. Butler, A. Haeberlen, M. Sherr, and W. Zhou, "Let sdn be your eyes: Secure forensics in data center networks," in *Proceedings of the NDSS workshop on security of emerging network technologies (SENT14)*, 2014.

[20] E. Casey, G. Back, and S. Barnum, "Leveraging cybox to standardize representation and exchange of digital forensic information," *Digital Investigation*, vol. 12, pp. S102–S110, 2015.

[21] J. M. de Fuentes, L. González-Manzano, A. I. Gonzalez-Tablas, and J. Blasco, "Wevan–a mechanism for evidence creation and verification in vanets," *Journal of Systems Architecture*, vol. 59, no. 10, pp. 985–995, 2013.

[22] R. Van Baar, H. Van Beek, and E. van Eijk, "Digital forensics as a service: A game changer," *Digital Investigation*, vol. 11, pp. S54–S62, 2014.

[23] K.-K. R. C. Daniel Jacob and N.-A. Le-Khac, "Volkswagen entertainment system forensics," in *16th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom 2017)*, IEEE. Sydney (Australia): IEEE, 08/2017 2017.