université PARIS-SACLAY

INSTITUT POLYTECHNIQUE DE PARIS

montimage

THESIS: SECURITY TESTING AND MONITORING OF CLOUD NATIVE 5G NETWORKS

Presented by Zujany Salazar

Supervised by:
Ana R. Cavalli, IP-Paris
Fathia Zahid, LRI, Université Paris-Saclay
Wissam Mallouli, Montimage

**Thesis CIFRE in the process of validation*

CONTEXT: 5G NETWORKS

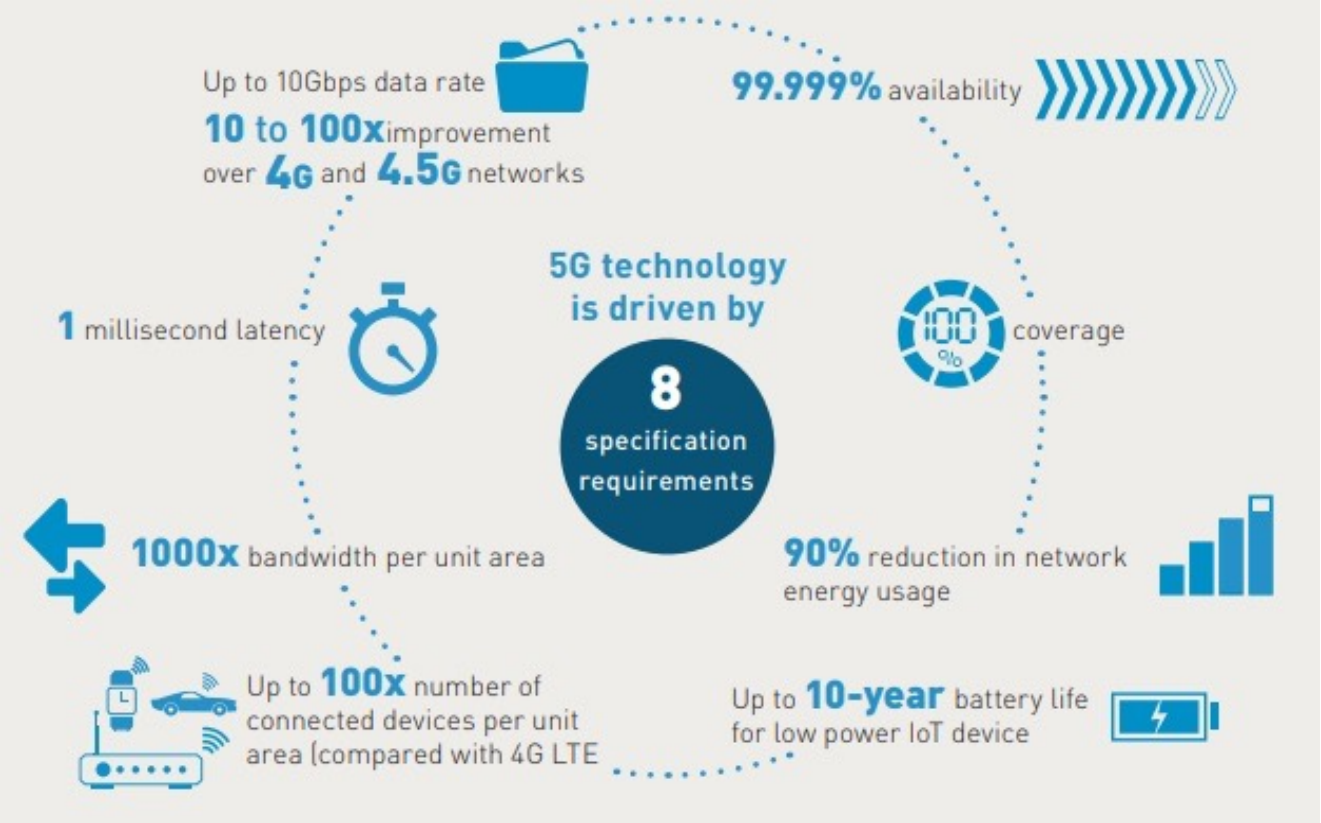


Figure 1. 5G KPIs[1]

1. *5G technology and networks (speed, use cases, rollout)*. Thales Group

5G ENABLING TECHNOLOGIES

1. Software defined networks (SDN)
2. Network functions virtualization (NFV)
3. Mobile Edge computing (MEC)
4. Network Slicing (NS)

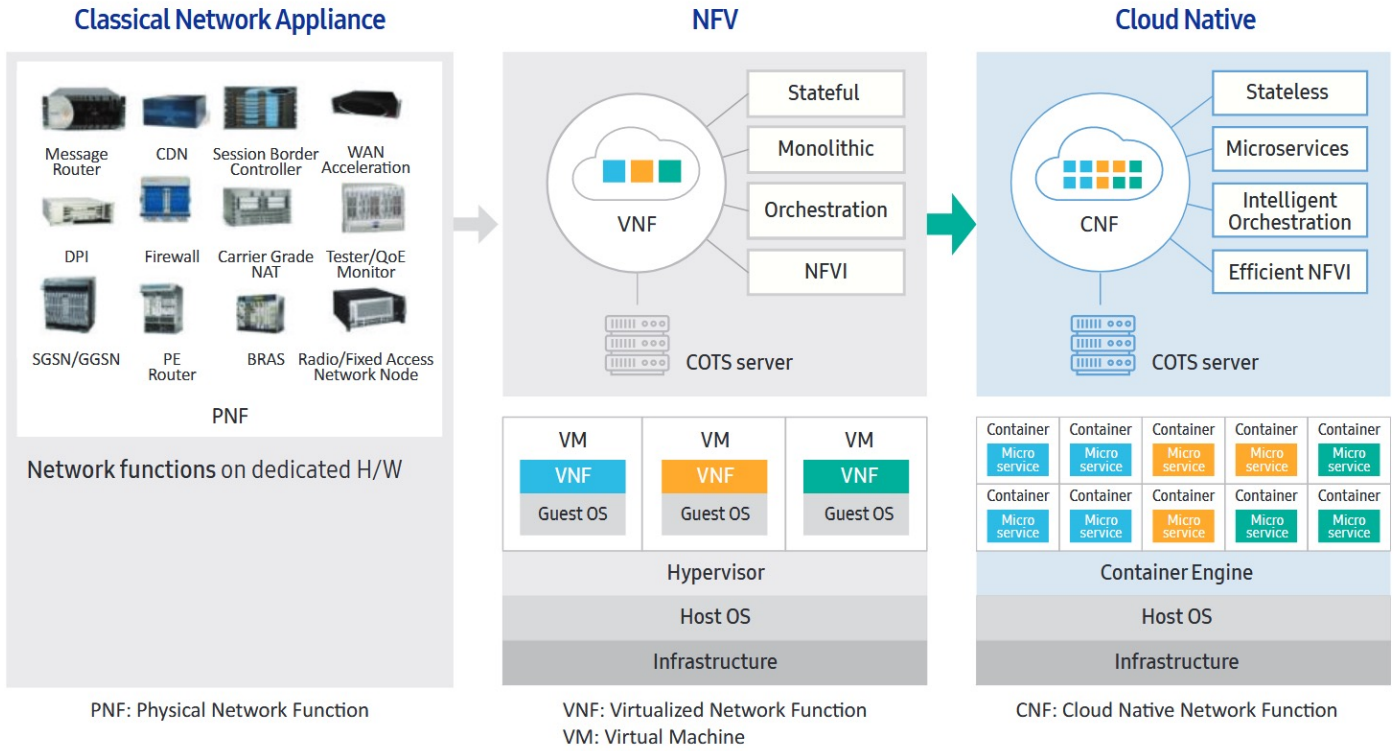


Figure 2. Evolving from dedicated hardware to cloud native architecture[1]

1. *Samsung 2020*

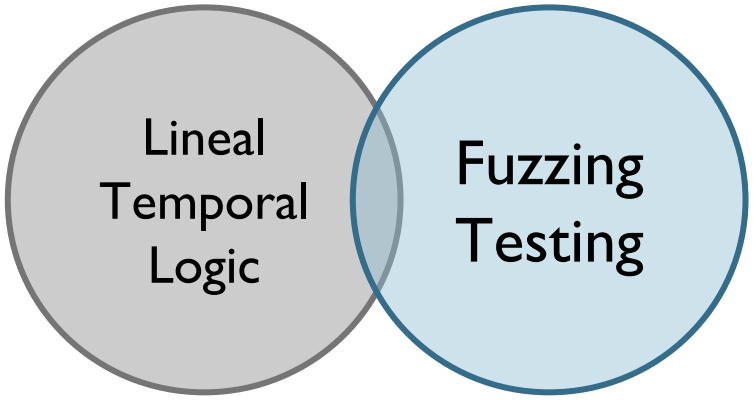
STATE-OF-THE ART
5G SECURITY CHALLENGES

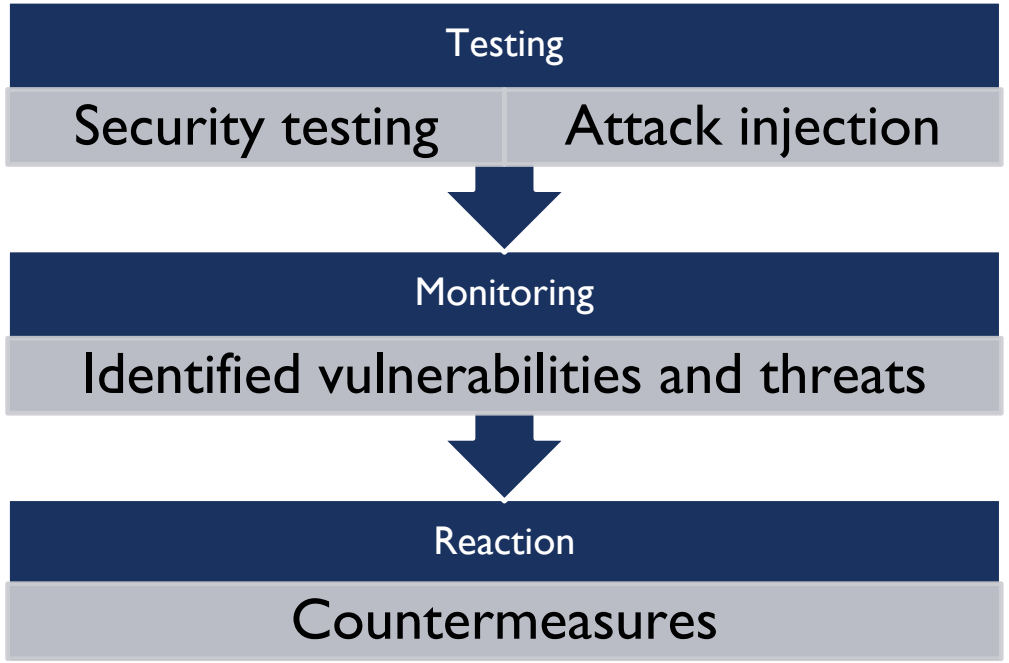
- New set cybersecurity issues (threats, vulnerabilities, attacks…)[1,2,3,4,5,6]
  - Vulnerabilities of 5G Core protocols
  - Vulnerable mechanisms for authentication and authorization of SDN components
  - Software Vulnerabilities in NFV implementation
  - Improper slice-authentication mechanisms
- Previous protection mechanisms not applicable to the new architecture[7]

1. *3GPP TS 33.512*
2. *ETSI GS NFV-SEC 013*
3. *A guide to 5G network security. Ericsson*
4. *5G Standalone core security research. Positive Technologies*
5. *ENISA threat landscape for 5G Networks*
6. *David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. 2018. A Formal Analysis of 5G Authentication. Proceedingsofthe2018ACMSIGSACConferenceonComputerandCommunicationsSecurity(2018)*
7. *Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov. 2018. Overview of 5G Security Challenges and Solutions. IEEE Communications Standards Magazine 2, 1 (2018), 36–43.*

OBJECTIVE
SECURITY TESTING AND MONITORING

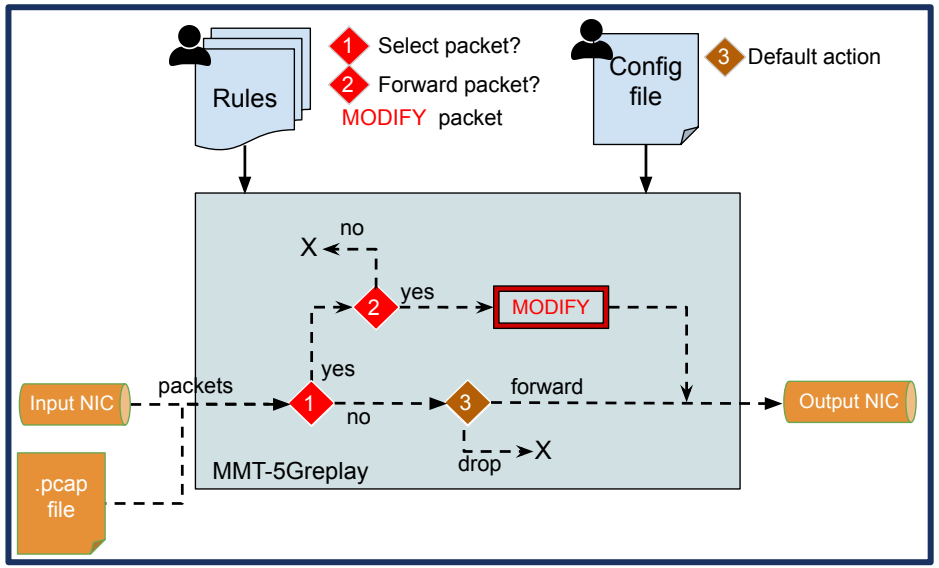
- Testing
- Identify threats and vulnerabilities





ON-GOING WORK – FIRST 6 MONTHS
5GREPLAY: A 5G NETWORK TRAFFIC FUZZER

5Greplay



Invalid, unexpected, random inputs*

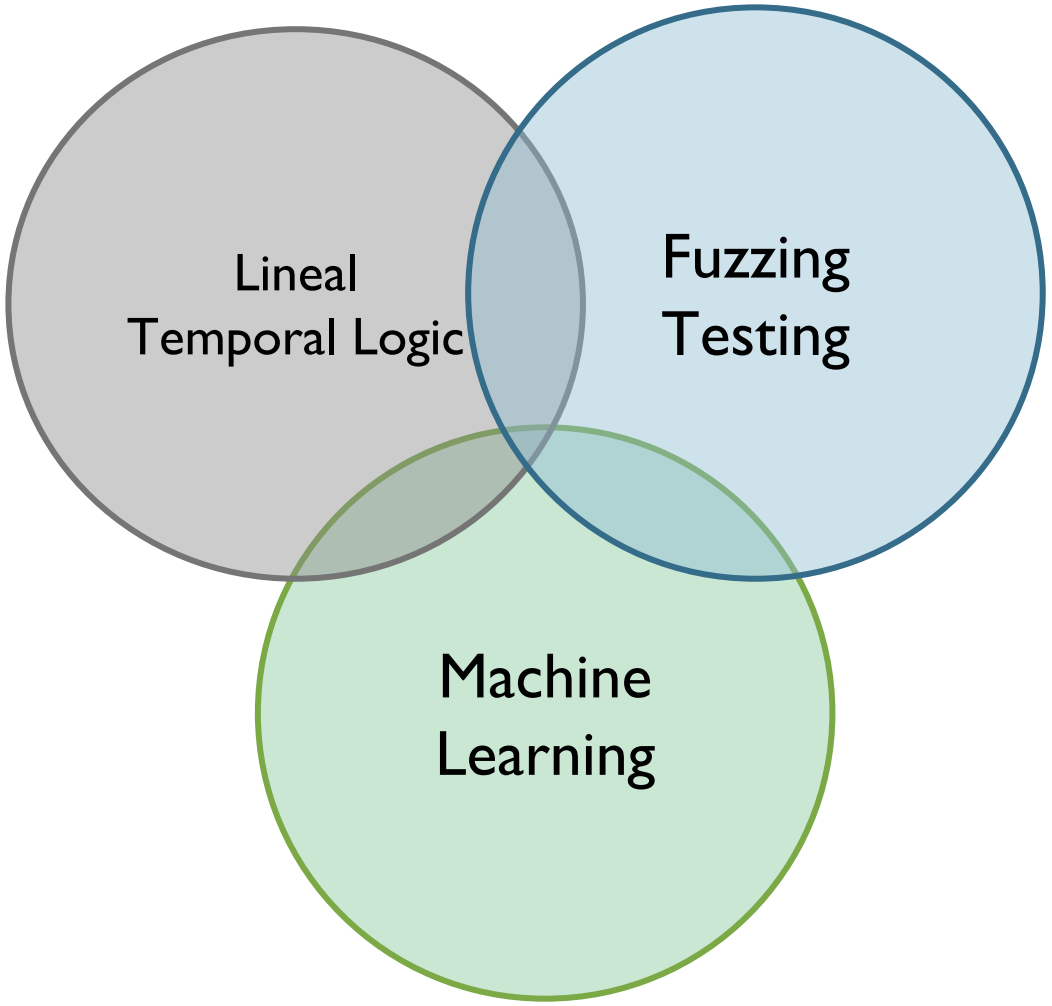
Complex attacks scenarios

Inside the target input domain*

5G VNF (e.g. AMF, UPF, SMF…),
5G IDSs,
5G applications…

PERSPECTIVES

- ML-based Fuzzer
  - Training dataset: pcap file with standard traffic. To learn the expected sequence of messages
  - While generating the output traffic, the fuzzer could take the learnt model to define the next packet to be sent
- Perfect learning technique -> always generate well-formed packets
- "Bad" learning techniques -> generate malformed packets that would be quickly dropped
- Find algorithm with adequate performance
- Generate a large set of test cases and increase their coverage



THANK FOR YOU ATTENTION

FOR QUESTIONS AND COMMENTS …

COME TO MY POSTER!