Threat Intelligence for 5G IoT

Prof. Thanh van Do, Telenor Research
IoT Week, Dublin 20-23 June 2022
Introduction

• As 5G strives to accomplishing its mission of supporting a multitude of IoT verticals it will be exposed to a big threat:

  **Flooding/DDOS attacks by IoT devices** that could lead to network breakdown and total service disruption

• Unfortunately, there is currently no adequate defense measure to protect the mobile network against Flooding attacks

• We present here a Flooding prevention solution proposed by Telenor, Wolffia and OsloMet experimented at the 5G4IoT Lab at OsloMet in the scope of the H2020 Concordia Project

• The solution will be able to detect Flooding attacks even before they are launched by using Threat Intelligence with Machine Learning
Why preventing Flooding Attacks

• The 5G network is a critical infrastructure for a variety of IoT verticals:
  • Emergency network and services
  • Smart city
  • eHealth
  • Intelligent transport
  • Defence/Army network
  • etc.
• A disruption in the 5G network will have severe consequences for the society
Is Flooding a real threat?

- Not yet happening but will happen if nothing is done

What drives 5G Security?

- New Verticals
- Threat landscape
- New tech
- Regulation

A wider perspective on 5G security
Huge threat from billion IoT devices

• Indeed, if billion of IoT devices get «mad» and bombard with messages the 5G network may collapse
• IoT devices are quite exposed
  – Could be tampered or hijacked without the knowledge of the owner
  – Simple and not capable of strong encryption and authentication
  – Unsecure communication
• Also, it is uncertain «who»/ «what» is behind an IoT device
  – It could be a simple primitive device
  – It could be a «monster» super computer
• The biggest challenge is that once detected a Flooding attack is almost unstoppable and the network may have already collapsed
A simple but genius solution

• If it is too late to wait until a Flooding attack is launched
• Then let’s detect and block it before
• The big question is: HOW?
• OUR SOLUTION is quite simple and assuming the following:
  • IoT devices used in a Flooding attack are compromised prior to an attack
  • They should have abnormal behaviour and activities
    – Communicating with alien parties
    – Have more activities than normal
  • On a fixed IP network it is not possible for the IoT platform and IoT owner to monitor and detect such anomalies
    – Because infected devices do not communicate with the IoT platform
  • On mobile networks, by collecting and analyzing data on the network layer both user and control data abnormal behaviours can be captured
Flooding vs DDoS attacks

**DDoS (Distributed Denial-of-Service)**
- Attempt to make it impossible for a service to be delivered to its intended users.
- By preventing access to virtually anything: servers, devices, services, networks, applications, and even specific transactions within applications
- Targeting a specific service provider or web site
- Detection can be done by analysis of traffic destined to a specific destination

**Flooding**
- Attempt to tear down the entire network blocking every service on the network
- Send a massive amount of traffic onto a specific network segment with the goal of creating so much network congestion that legitimate traffic cannot reach the target server or service.
- This type of attack is not specific to any Web site as the traffic sent onto the network could really be of any type
- Detection
Flooding attacks on mobile networks

- Aims at taking down the entire mobile network:
  - No phone call
  - No SMS
  - No emergency call

- Blocking Radio Access Network (RAN)
- Blocking Control Plane
- Blocking Data Plane
The Detection of Flooding Attacks solution

• Collection and analyse of data at three locations:
  • On the application layer
  • On the Network layer:
    – User plane
    – Control plane
The 5G4IoT Machine Learning Platform

• Making use of Machine Learning
• Semi-supervise
• Both labelled and unlabelled data
• Benign (normal) data are used to build a profile of the normal situation
• Any deviation is interpreted as an anomaly that will be analysed by security experts

• A big challenge: The lack of malicious data
• Solutions:
  – Simulated attacks with purposely infected devices
    • Simulated Mobile phones
    • Raspberry PI infected with Mirai
  - Generation of traffic based collected traffic
Achievements

• A 5G IoT testbed is established at the 5G4IoT lab:
  • A small lab 5G network is built with:
    – Commodity computers combined with OsloMet cloud
    – Using USRP (Universal Software defined Radio Peripheral)
    – Running OpenAirInterface and Open5GS
  • A variety of devices:
    – Mobile phones
    – Digital locks
    – Cameras
    – Raspberry Pis
    – Sensors
  • A ML platform based on commodity computers and open source software
  • Profiles for normal situation have been built
• Next step: Introduce anomalies:
  • Particular app on mobile phones
  • Simulated infected Raspberry Pi
Conclusion

• IoT will play a central role in the digitalization of the society
  • More and more devices and sensors will be used
  • More security will be needed to ensure that these IoT devices are functioning as intended
• 5G will be the dominant connectivity and communication infrastructure which has the critical mission to support and provide adequate security to IoT applications and devices
• With the rise of AI/ML it is natural that AI/ML should be used to provide improved security for IoT but the main challenge is the data sets:
  • What are the relevant data?
  • Where/How to collect them?
  • How to store and consume them?
• Another challenge is how to share the lessons learnt between mobile networks:
  • Due to differences in size, distribution, number of users, configuration, etc.
• We will continue researching to bring clarity to these issues
Thank you
Differences with DDoS attacks on fixed networks

• Attacks can be launched on the application layer, on the network user plane or control plane or on the RAN

• Attacks can happen before the devices get allocated an IP address:
  • Other mobile identities must be used:
    – **SUPI** - Subscription Permanent Identifier
      • **IMSI** – International Mobile Subscriber Identity
    – **SUCI** - Subscription Concealed Identifier
    – **GUTI** – Global Unique Temporary Identifier
      • **TMSI** – Temporary Mobile Subscriber Identity
    – **PEI** – Permanent Equipment Identifier
    – **DNN** - Data Network Name
    – **NSSAI** - Network Slice Selection Assistance Information

• Mobility of devices
  • Change in device location and concentration
  • Registration Area/Tracking Area is a relevant attribute

• Unknown an uncontrolled number of devices connected to the mobile network
  • Roaming devices from other mobile networks

• Protocols and collected data sets are different
5G User Plane Protocol stack
5G Control Plane Protocol Stack
L3 Signalling Message

• A standard L3 message consists of:
  • an imperative part, itself composed of a header and the rest of imperative part
  • followed by a non-imperative part.
  • Both the non-header part of the imperative part and the non-imperative part are composed of successive parts referred as standard information elements.
• Totally four categories of standard information elements (IE) are defined:
  • information elements of format V or TV with value part consisting of 1/2 octet (type 1);
  • information elements of format T with value part consisting of 0 octets (type 2);
  • information elements of format V or TV with value part that has fixed length of at least one octet (type 3);
  • information elements of format LV or TLV with value part consisting of zero, one or more octets (type 4)
Non-Access-Stratum (NAS) message for 5G System

- Every 5GS NAS message is a standard L3 message
- NAS message categories:
  - Registration
  - Call Control
  - Call independent Supplementary Services
  - Short Message Service
  - Session Management Service
  - Location services

General message organization example for a plain 5GS NAS message
Mobile Station Call Control state

two thousand computers were infected within fifteen hours.
Data Capture

- Using Wireshark installed at the gNB and 5G/4G Core
- With the following filters:
  - nas-5gs: Non-Access-Stratum 5GS (NAS) PDU (2.6.0 to 3.4.0, 358 fields)
  - nas-eps: Non-Access-Stratum (NAS) PDU (1.2.0 to 3.4.0, 365 fields)
  - gtp: GPRS Tunneling Protocol (1.0.0 to 3.4.0, 354 fields)
  - gtpv2: GPRS Tunneling Protocol V2 (1.2.0 to 3.4.0, 738 fields)
- Generating csv files
- Fine tuning and removing irrelevant parameters
- Aggregating and feeding to the Machine Learning Platform
Research Challenges

• When the ML learning platform detects an outlier i.e. abnormal situation which is found to be an attack by a security expert can this outlier be transformed to an Indicator of Compromise to be shared in MISP:
  • An outlier is a deviation from on a normal situation profile which is modelled by complex algorithm and may not be transformed to an IoC
  • A normal situation of one network is different from others: number and types of subscription, traffic, configuration, etc.
• Conversely, it may also be challenging to use IoC in the training of the ML Platform
• How can experiences/lessons learned from the fixed network can be used in the mobile network? And Vice versa?