Report

제출일	2021.12.01
과목명	Cyber Security
담당교수	한명묵 교수님
팀명	Team 10
팀원	201533673 최준헌
	201835462 박해원
	201835521 정현서

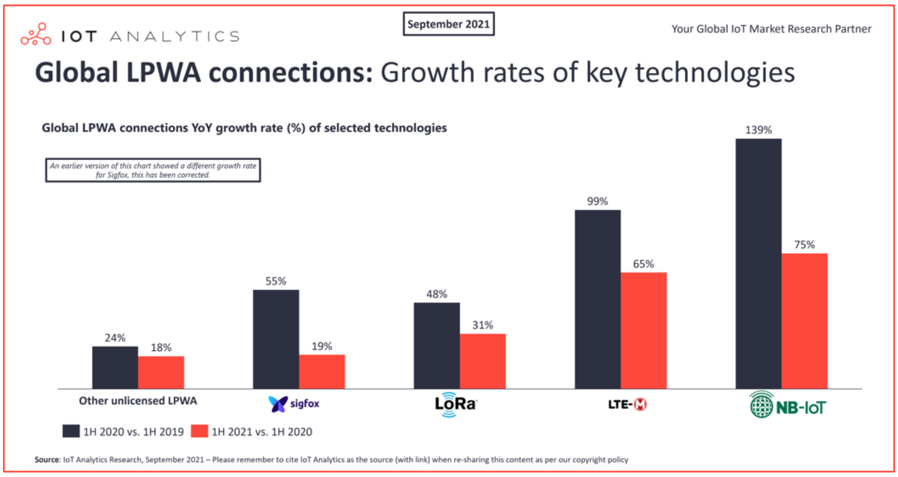
AI-Powered Network Security

(Wireless Communications and Security), Prof. Elisa Bertino

NextGen Wireless System

NextGen wireless systems will support novel forms of societal communications, applications, and trends.

- Holographic communications and haptic internet applications
- Connectivity for everything, including internet of Bio-nano things (IoBNT)
- Chip-to-chip communications and nanonetworks
- Industry 4.0



According to the statistics above, NextGen wireless systems will be more about connecting devices, autonomous systems, robots than just humans via cell phones. Also, NextGen Wireless Systems will be increasingly complex and be part of even more complex network systems, mobile phones and devices will support an increasing diversity of wireless technologies. And many different types of mobile operators.

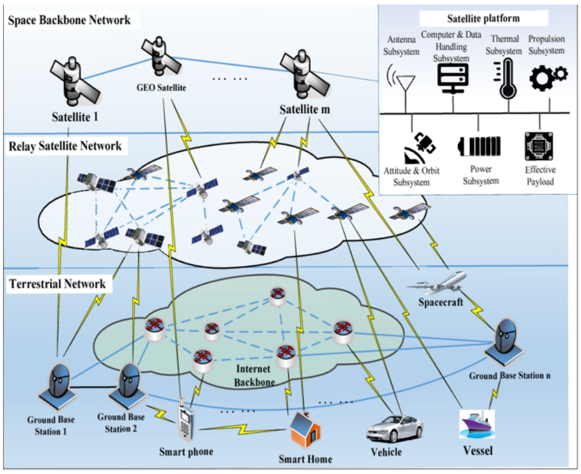
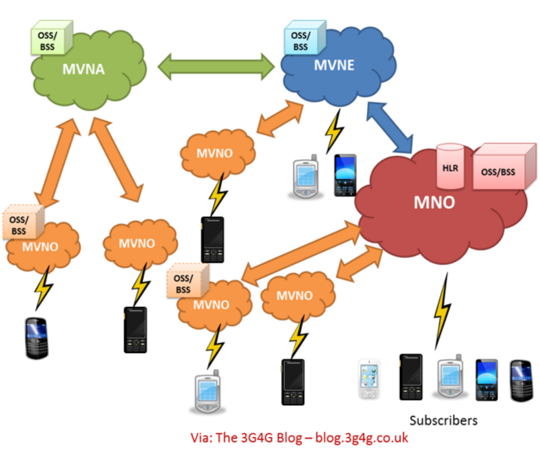


FIGURE 1. Typical architecture of a satellite communication network



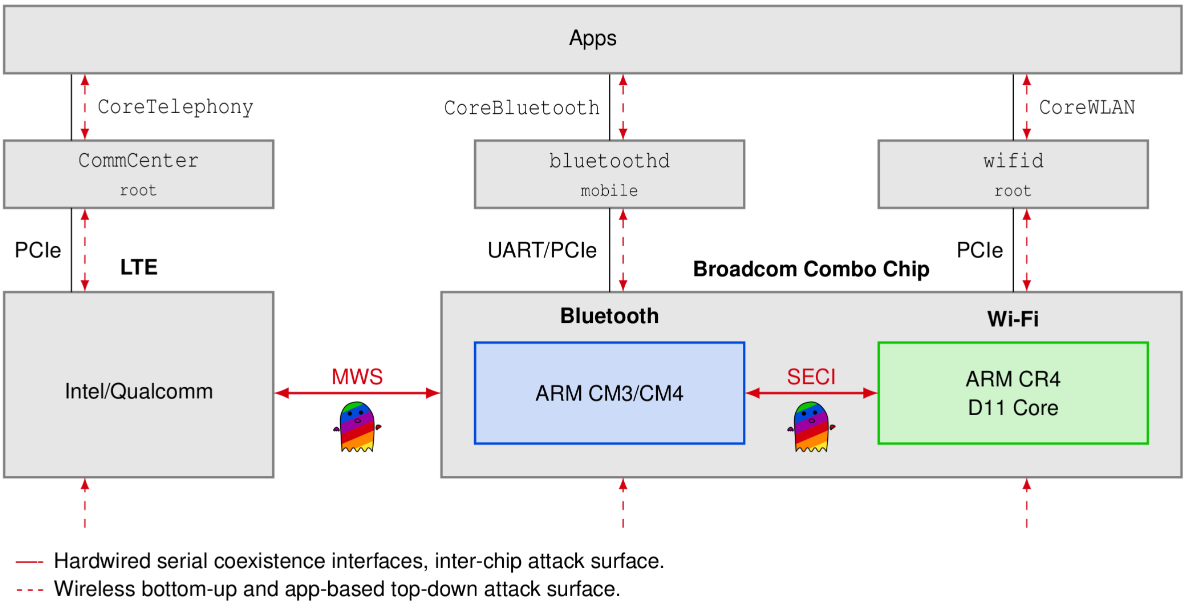
Via: The 3G4G Blog – blog.3g4g.co.uk

Complexity is the Enemy of Security - Examples

1. Spectra: Inter-chip privilege escalation using wireless coexistence Mechanisms by J. Classen and ai (BlackHat USA 2020)

   [Vulnerabilities examples]

   - Reconfiguring the SECI via Bluetooth causes a voltage drop, which in turn stops WIFI and halts the processor communication to the WIFI.
   - The WIFI core shares parts of its RAM to the Bluetooth core, leaking sensitive information.

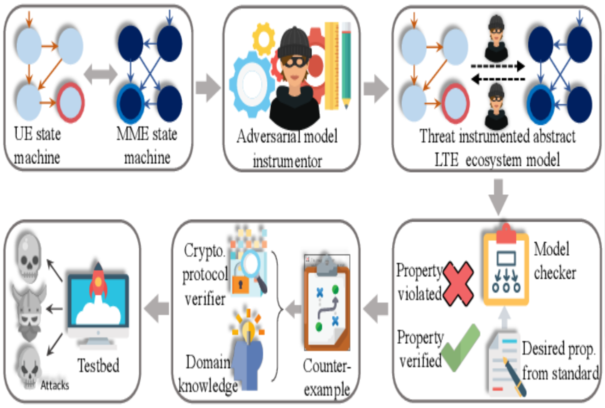


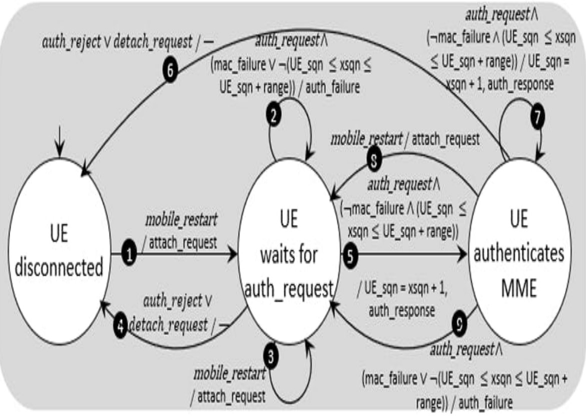
2. VoLTE and VoWiFi

   [Initial results]

   - On certain phone models, when VoWiFi is being used, attacks to VoWiFi prevent the phone from receiving calls on VoLTE.
   - The reason is that when VoWiFi is used, the phone doesn't execute the paging protocol on the cellular network.

How Can Address Security?


UE state machine
MME state machine
Adversarial model instrumentor
Threat instrumented abstract LTE ecosystem model
Model checker
Property violated
Property verified
Desired prop. from standard
Crypto. protocol verifier
Domain knowledge
Counter-example
Testbed
Attacks


auth_reject ∨ detach_request / —
6
auth_request∧ (mac_failure ∨ ¬(UE_sqn ≤ xsqn ≤ UE_sqn + range)) / auth_failure
2
auth_request∧ (¬mac_failure ∧ (UE_sqn ≤ xsqn ≤ UE_sqn + range)) / UE_sqn = xsqn + 1, auth_response
7
mobile_restart / attach_request
8
auth_request∧ (¬mac_failure ∧ (UE_sqn ≤ xsqn ≤ UE_sqn + range))
UE disconnected
mobile_restart / attach_request
1
UE waits for auth_request
5
UE authenticates MME
/ UE_sqn = xsqn + 1, auth_response
auth_reject ∨ detach_request / —
4
9
auth_request∧ (mac_failure ∨ ¬(UE_sqn ≤ xsqn ≤ UE_sqn + range)) / auth_failure
3
mobile_restart / attach_request

1. Network Security Foundations
2. Network Security Lifecycle

   ① Prepare and Prevent

   - Learning and deploying network security policies
   - Assuring correctness of network "programs"

   ② Monitor and Detect

   - Network monitoring for anomaly detection
   - Network monitoring for identifying devices connected to the network

   ③ Diagnose and Understand

   - Identifying attack points and affected network portions
   - Predicting possible next steps of the attack
   - Combining two ML models for protecting against DoS attacks

     i. One model predicts signaling workload.

     ii. The other model determines if the predicted workload has anomalies.

   ④ React, Recover and Fix

   - Taking actions to contain the attack
   - Taking steps to bring back the network to the "normal" state
   - Permanently removing the vulnerabilities exploited by the attack
   - Using Reinforcement Learning to slow down potentially malicious flows.

Zero Trust Architecture (ZTA)

The goal of this architecture is to secure sensitive data, systems, and services hosted in a given enterprise or organization. As well as this model assumes that “no actor, system, network, or service operating outside or within the security perimeter is trusted”. Also, this model is “is a dramatic paradigm shift in philosophy of how we secure our infrastructure, networks, and data, from verify once at the perimeter to continual verification of each user, device, application, and transaction”.

ABAC Policies

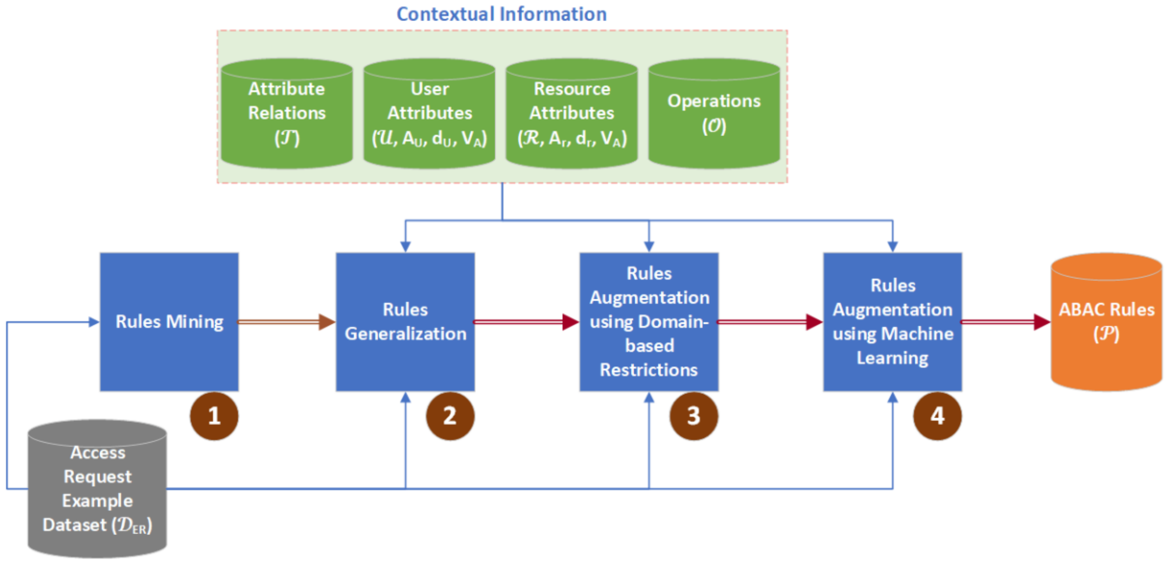
ABAC policies are specified as Boolean combinations of conditions on attributes of users and protected resources.

If assume Users($\mathcal{U}$), Operations($\mathcal{O}$), Resources($\mathcal{R}$), Polices($\mathcal{P}$), User Attributes(A_U), User Attribute Expression(e_U), Resource Attributes(A_R), Resource Attribute Expression(e_R), the following formula will hold.

$$A\ rule\ p \in \mathcal{P} < e_U, e_R, O, d >$$
$$O \subseteq \mathcal{O}, d \in \{permit, deny\}$$

Polisma

1. Pipeline


Contextual Information
Attribute Relations ($\mathcal{T}$)
User Attributes ($\mathcal{U}$, A_U, d_U, V_A)
Resource Attributes ($\mathcal{R}$, A_r, d_r, V_A)
Operations ($\mathcal{O}$)
Rules Mining
Rules Generalization
Rules Augmentation using Domain-based Restrictions
Rules Augmentation using Machine Learning
ABAC Rules ($\mathcal{P}$)
1
2
3
4
Access Request Example Dataset ($\mathcal{D}_{ER}$)

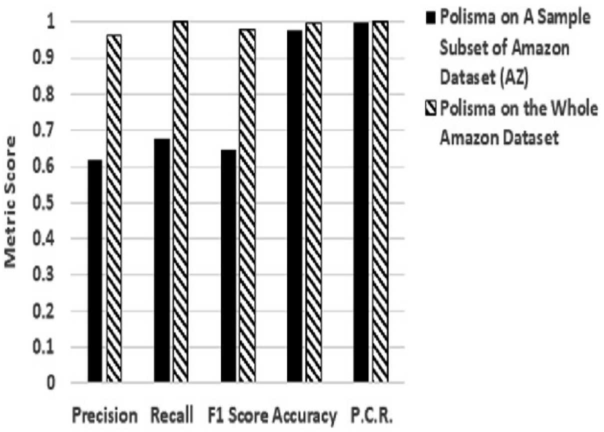
① Rules Mining

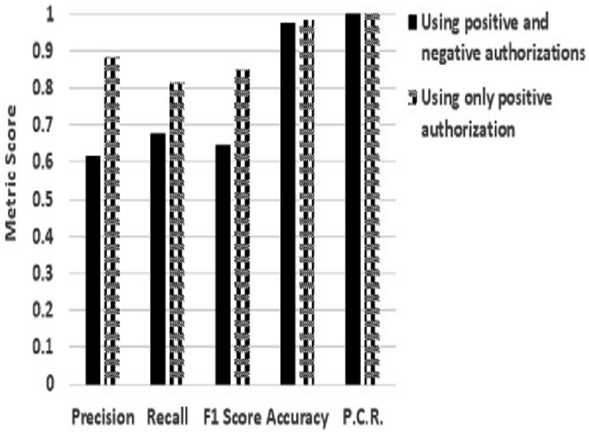
② Rules Generalization

③ Rules Augmentation using Domain-based Restrictions

④ Rules Augmentation using Machine Learning

2. Experimental results





On the whole Amazon dataset (700k decision examples), Polisma achieves significantly improved scores compared to those when suing the AZ dataset (a sample of 1k decision examples) because Polisma was able to utilize a larger set of decision examples. Nonetheless, given that the size of AZ was small compared to that of the whole Amazon dataset, Polisma outcomes using AZ are promising. When considering only positive authorizations, the results improve significantly. This is since the negative examples are few and so they are not sufficient in improving the learning of negative authorizations.