5G Vulnerability Analysis with Reinforcement Learning Toolbox

MathWorks Expo

05/18/2022

Ambrose Kam

LOCKHEED MARTIN

5G SECURITY DIMENSIONS

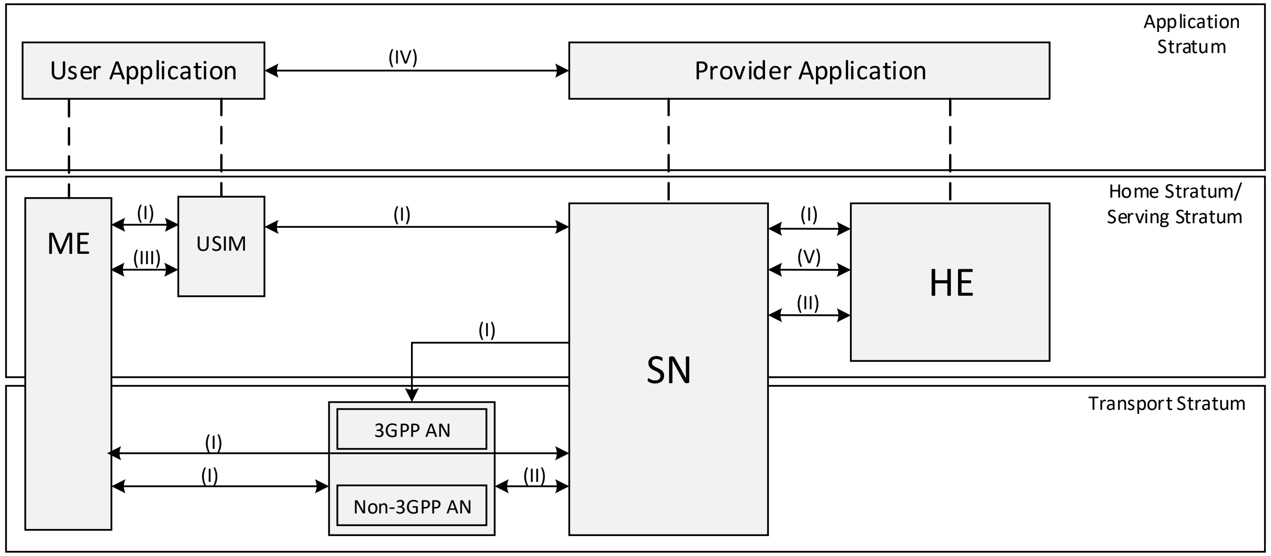
- The International Telecommunication Union Standardization Sector (ITU-T) has recommended consideration of 8 "security dimensions"
- These dimensions provide specific nomenclature and scope of security elements for protection against all major security threats
- These dimensions consider security threats relevant to the network, applications and user data
- The vision is for 5G to ultimately have built-in security, flexible security and automated security (e.g., employing artificial intelligence)
- Recommendations include addressing 5G security early in the design process

Security Dimension	Brief Explanation
Access Control	Protects against unauthorized use of network resources. It also ensures that only authorized persons or devices access the network elements, services, stored information and information flows.
Authentication	Confirms identities of communicating entities, ensures validity of their claimed identities, and provides assurance against masquerade or replay attacks.
Non-Repudiation	Provides means for associating actions with entities or user using the network and that an action has either been committed or not by the entity.
Data Confidentiality	Protects data from unauthorized disclosure, ensures that the data content cannot be understood by unauthorized entities.
Communication security	Ensures that information flows only between the authorized end points and is not diverted or intercepted while in transit.
Data integrity	Ensures the correctness or accuracy of data, and its protection from unauthorized creation, modification, deletion, and replication. It als provides indications of unauthorized activities related the data.
Availability	Ensures that there is no denial of authorized access to network resources, stored information or its flow, services and applications.
Privacy	Provides protection of information that might be derived from the observation of network activities.

Source: "Security architecture for systems providing end-to-end communications," Int. Telecommun. Union, Geneva, Switzerland, ITU-Recommendation X.805, 2003.

THE 5G SECURITY FRAMEWORK

- **The 5G Security Framework specification is established in 3GPP R15**
  - This framework establishes the architecture, nomenclature and high-level procedures for the 5G System
  - Six distinct 5G Security Domains are defined (see below)
  - The framework does *not* specify specific threats or remedies



5G Security Domains

I Network Access Security
II Network Domain Security
III User Domain Security
IV Application Domain
V Service Based Architecture Domain Security
VI Visibility and Configurability

Source: 3GPP, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 15)," 3GPP TS 33.501 v15.3.1, Dec 2018

Acronyms: Mobile Equipment (ME) | Universal Subscriber Identity Module (USIM) | Serving Network (SN) | Home Environment (HE) | Access Network (AN)

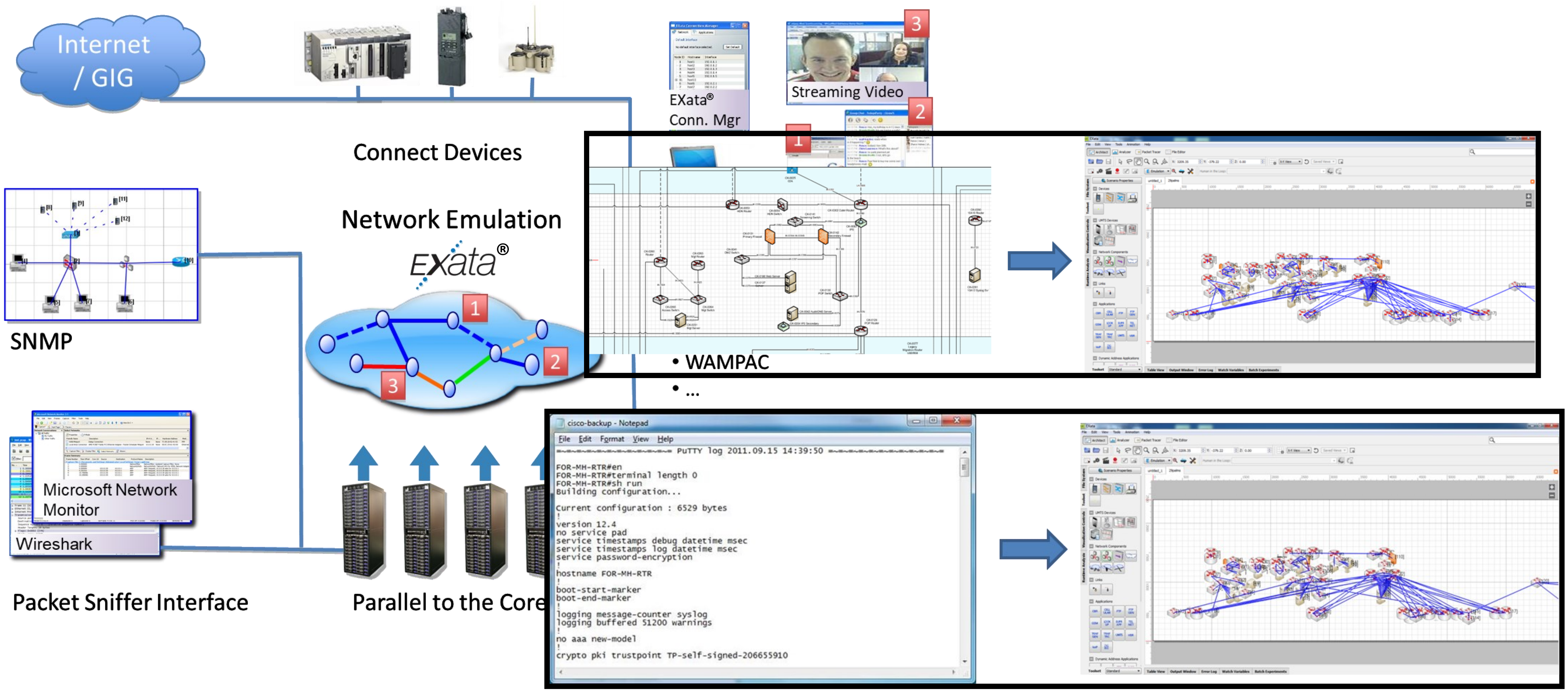
SECURITY CHALLENGES IN 5G NETWORK SEGMENTS

- **A summary of known security threats and potential targets in 5G is provided in the table below, including an indication of the affected network segments**

Security threats	Potential targets	Affected network segments		
		HetNet Access	Backhaul	Core Network
DoS attack on signaling plane	Centralized control elements			✓
Hijacking attacks	SDN controller, hypervisor	✓	✓	
Signaling storms	5G core network elements			✓
Un-authorized access	Low-power access points	✓		
Configuration attacks	Low-power access points	✓		
Saturation attacks	Ping-pong behavior in access points, and MME	✓		✓
Penetration attacks	Subscriber information			✓
User identity theft	User information data bases			✓
Man-in-the middle attack	Un-encrypted channels, e.g. in IoT	✓		
TCP level attacks	Gateways, router and switches		✓	
Key exposure	Radio interfaces	✓		
Session replay attacks	Session keys in non-3GPP access	✓		
Reset and IP spoofing	Control channels	✓		
Scanning attacks	Radio interfaces interfaces	✓		
IMSI catching attacks	Roaming and UE	✓		
Jamming attacks	Wireless channels	✓		
Channel prediction attacks	Radio interfaces	✓		
Active eavesdropping	Control channels	✓		✓
Passive eavesdropping	Control channels	✓		✓
NAS signaling storms	Bearer activation in core network elements			✓
Traffic bursts by IoT	Saturation of GTP end-points		✓	✓

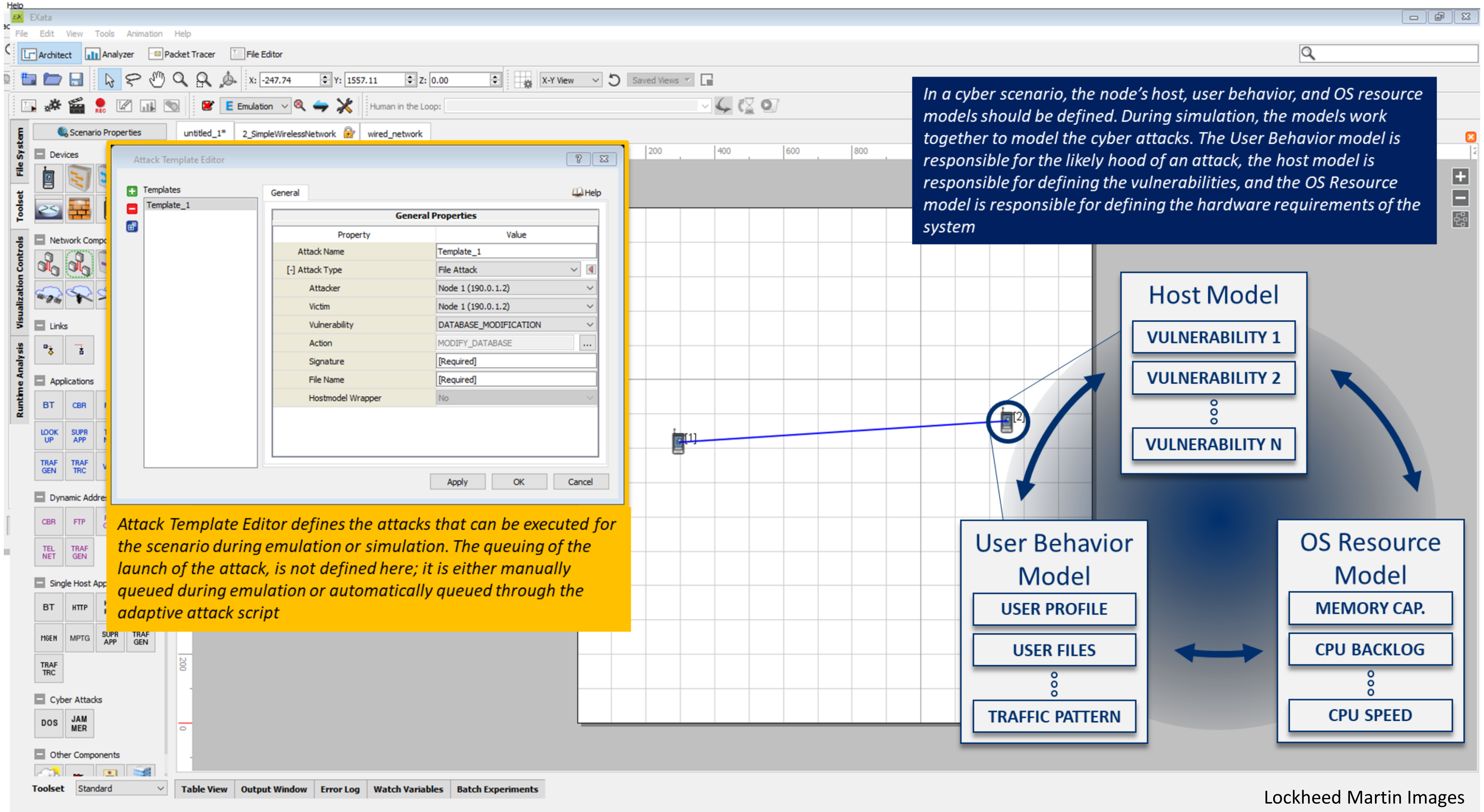
Source: "Security for 5G and Beyond." Ijaz Ahmad ; Shahriar Shahabuddin ; Tanesh Kumar ; Jude Okwuibe ; Andrei Gurtov ; Mika Ylianttila
IEEE Communications Surveys & Tutorials, Year: 2019 | Volume: 21, Issue: 4 | Journal Article | Publisher: IEEE

EXata®


Internet / GIG
Connect Devices
EXata® Conn. Mgr
Streaming Video
SNMP
Network Emulation
EXata®
• WAMPAC
• ...
Microsoft Network Monitor
Wireshark
Packet Sniffer Interface
Parallel to the Core
cisco-backup - Notepad
File Edit Format View Help
PuTTY log 2011.09.15 14:39:50
FOR-MH-RTR#en
FOR-MH-RTR#terminal length 0
FOR-MH-RTR#sh run
Building configuration...
Current configuration : 6529 bytes
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname FOR-MH-RTR
boot-start-marker
boot-end-marker
logging message-counter syslog
logging buffered 51200 warnings
no aaa new-model
crypto pki trustpoint TP-self-signed-206655910

Sample: 5G Vulnerability Modeling

LOCKHEED MARTIN



In a cyber scenario, the node's host, user behavior, and OS resource models should be defined. During simulation, the models work together to model the cyber attacks. The User Behavior model is responsible for the likely hood of an attack, the host model is responsible for defining the vulnerabilities, and the OS Resource model is responsible for defining the hardware requirements of the system

Attack Template Editor defines the attacks that can be executed for the scenario during emulation or simulation. The queuing of the launch of the attack, is not defined here; it is either manually queued during emulation or automatically queued through the adaptive attack script

Lockheed Martin Images

Sample: Cyber Attack Models

- The following is a list of EXata provided Cyber Attack models

- A Cyber Attack model may support launching through:
  1. **HITL Interface** *<u>prior</u> to enumeration/simulation*
  2. **Canvas in EXata® GUI** *<u>during</u> enumeration*
  3. **Canvas in Scenario Player** *<u>during</u> enumeration*
  4. **Attack History Manager in EXata® GUI** *<u>during</u> enumeration*
  5. **Adaptive Attack Scripts** *<u>during</u> enumeration*

- If a Cyber Attack model can be made into an **Attack Template**, the model can be launched from methods 2-5 *(EXata® GUI, Scenario Player, Attack History Manager, and Adaptive Attack Scripts)*

- Only certain Cyber Attack models can exploit a vulnerability, these models are identified in the table to the right

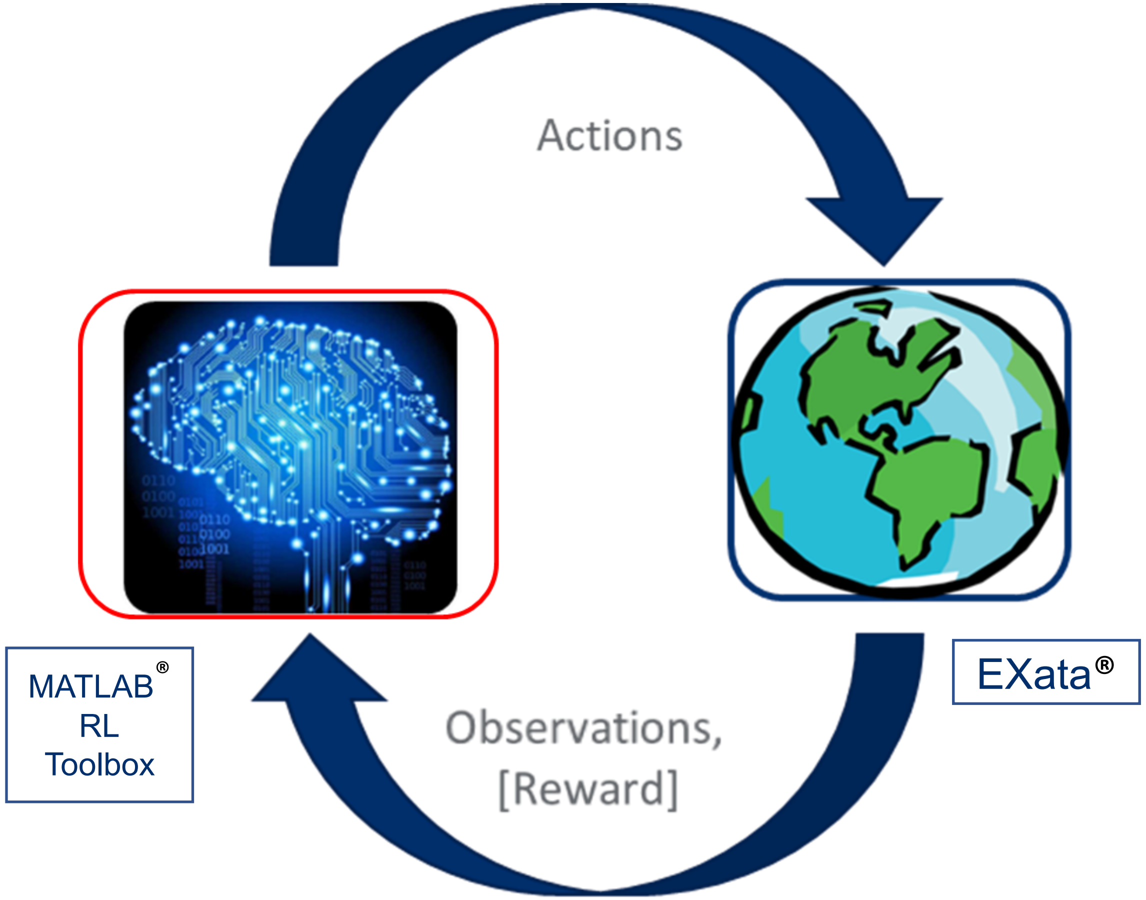
	HITL Compatible	Attack Template Compatible	Exploits Vulnerability
Botnet Worm and Botnet Virus Attacks*	⊖	⊖	⊖
Data Transfer Attacks	⊖	✓	⊖
Denial of Service (DOS) Attacks	✓	✓	⊖
Eavesdropping Attacks	✓	✓	⊖
File Attacks	⊖	✓	✓
Hacking Attacks	⊖	✓	✓
Jamming Attacks	✓	✓	⊖
Malware Virus Attacks	⊖	✓	✓
Malware Worm Attacks	⊖	✓	✓
Modify Packets Attacks	✓	✓	⊖
Network Scanning Attacks	✓	✓	⊖
Phishing Email Attacks	⊖	✓	⊖
Port Scanning Attacks	✓	✓	⊖
Ransomware Attacks	⊖	✓	⊖
Rootkit Attacks	⊖	✓	⊖
Signals Intelligence (SIGINT) Attacks	✓	✓	⊖
Generic Vulnerability Attack	⊖	✓	✓

Lockheed Martin Images

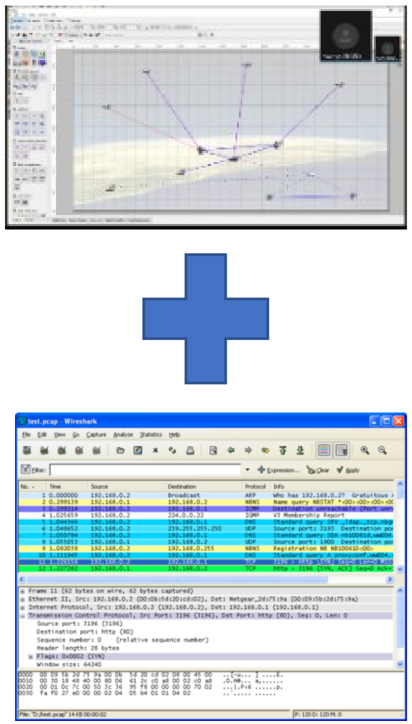
Botnet Worm and Botnet Virus Attacks can only be launched from the Canvas of the Scenario Player

Reinforcement Learning Adversarial Agent

LOCKHEED MARTIN

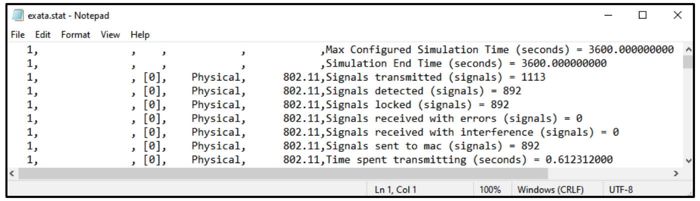


Network security
Firewalls
Port and network scanning
Eavesdropping
Jammers
Denial of Service
Packet Modification
Stimulate Intrusion Detection System
Signals Intelligence
Operating System resource models
Vulnerability exploitation
Virus attacks
Worm and virus propagation
Antivirus
Backdoors, rootkits
Host models
Botnets
Coordinated attacks
Adaptive attacks
Social media attacks
Ransomware
Data exfiltration

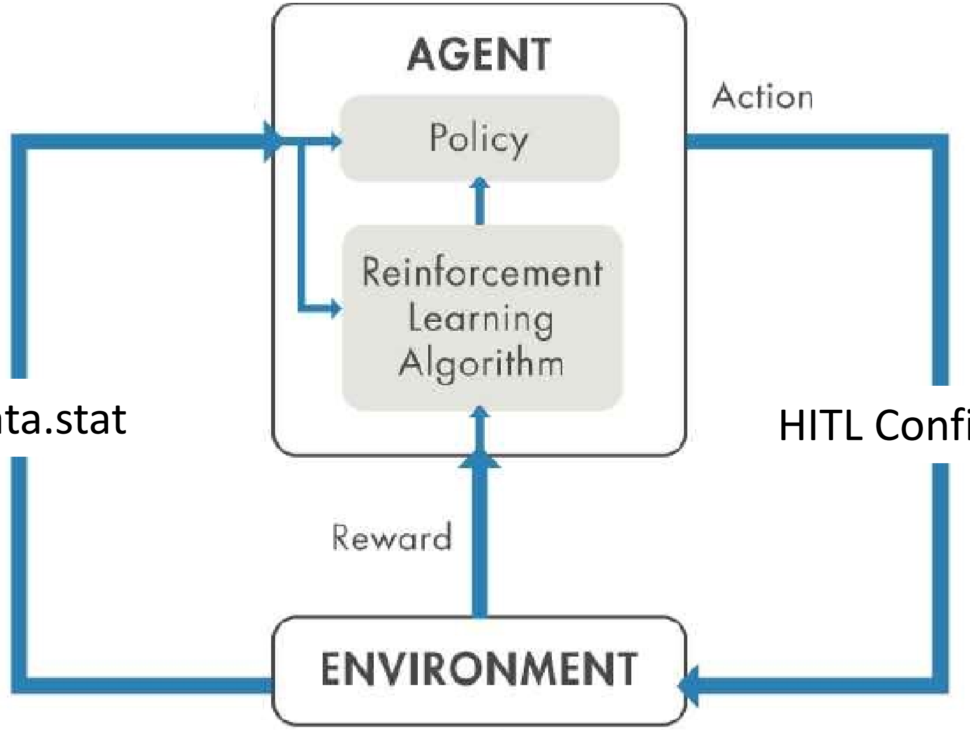


Lockheed Martin Images

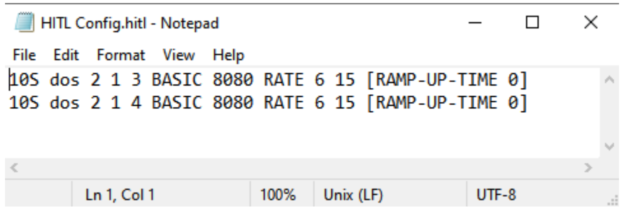
Training MATLAB® Agent with EXata®



exata.stat



HITL Config File



Lockheed Martin Images]

Training Results

3000
TOTAL EPISODES

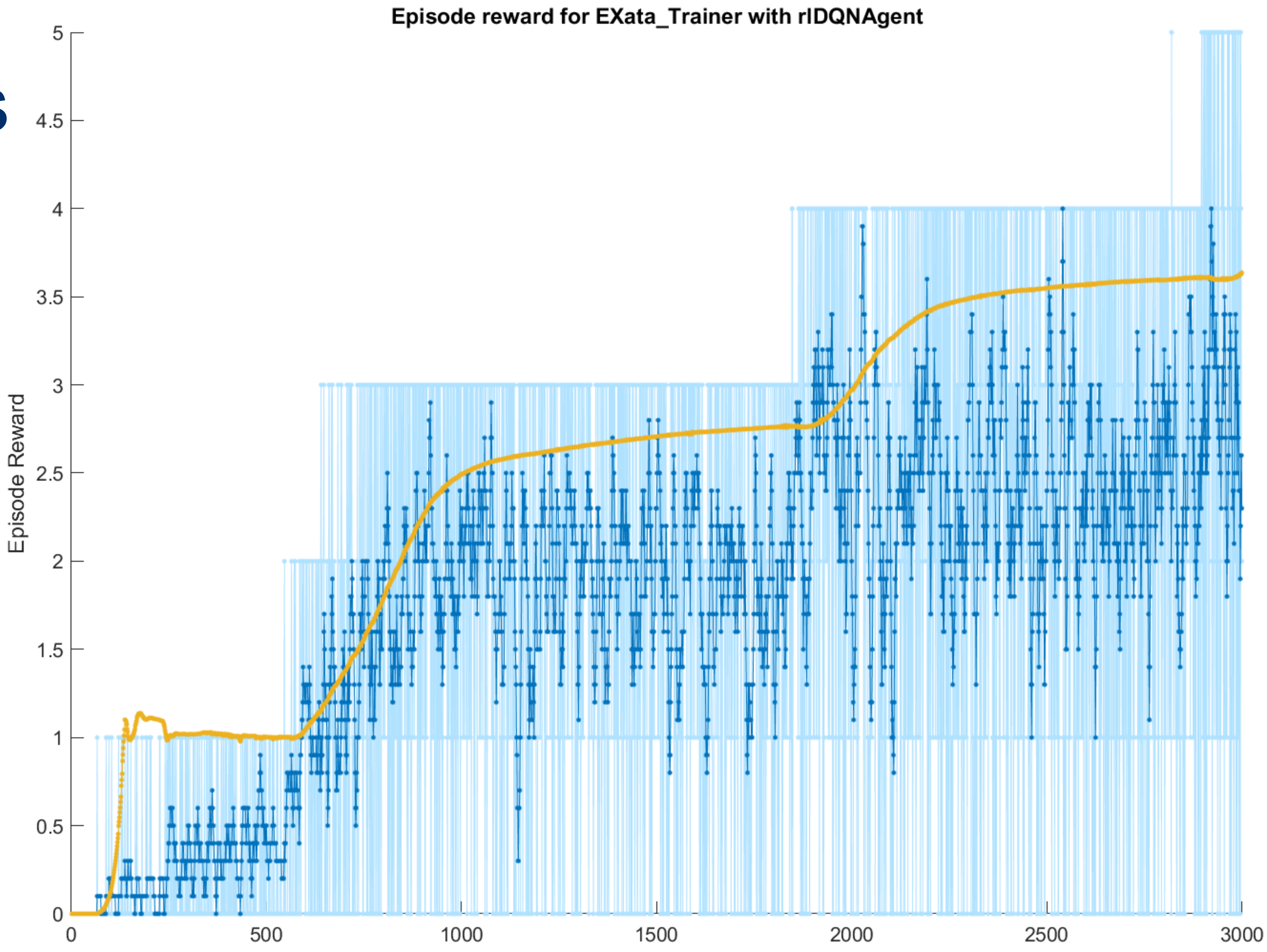
8246
TOTAL AGENT STEPS

5
MAXIMUM POSSIBLE REWARD

5
ACHIEVED REWARD

03:25:26
TRAINING DURATION

3.6365
EPISODE Q0

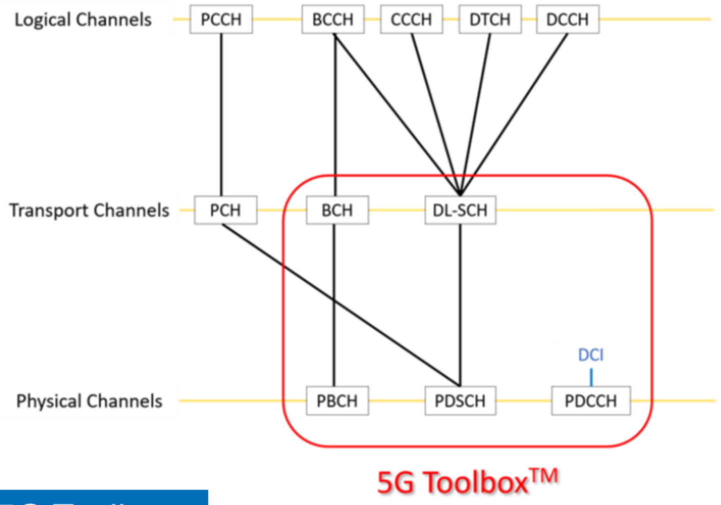


Lockheed Martin Images

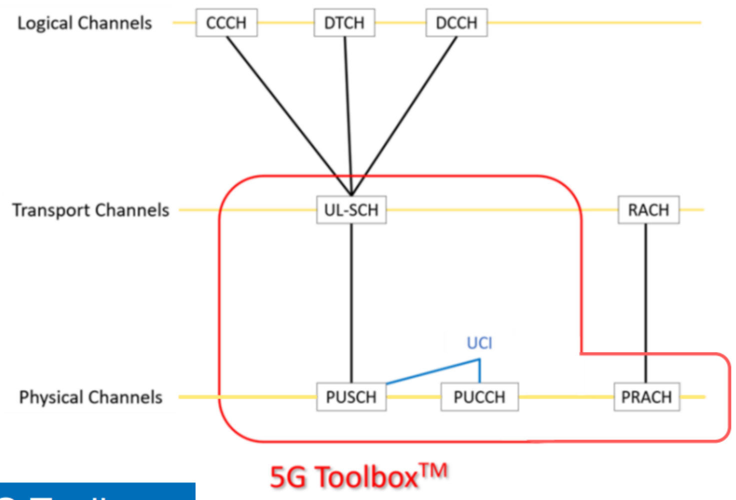
Future Work

LOCKHEED MARTIN

- **Transition to a multi-agent reinforcement framework (enabled by Simulink) for better realism**
- **Adapt industry standard (MITRE's ATT&CK & D3FEND) tactics and techniques**
- **Train/Execute agents using simulation tools like CANS and AFSIM**
- **Integrate with MATLAB® 5G Toolbox for better fidelity (PHY)**
- **Combine Cyber with EW effects**



Link: 5G Toolbox



Link: 5G Toolbox

Source: MathWorks, "5G with AI Starts Here," MathWorks, Dec 2021

MathWorks®

“Collaboration with a Purpose”

“Reinforcement Learning-based 5G Vulnerability Analysis”
Lockheed Martin Rotary & Mission Systems

Ambrose Kam, LM Fellow in Cyber Innovation, RMS Moorestown

Challenge:
5G is a disruptive technology that transforms our society. And yet, there are many potential attack vectors that threat actors could take advantage of. To better protect our critical infrastructure and the devices on them, we need to identify as many vulnerabilities as we can so they could addressed.

Obstacle:
A 5G infrastructure is comprised of many components and is being used in many different environments. The system complexity and dynamic nature of it add to the challenge of identifying vulnerabilities. Data security, user privacy, confidentiality, integrity and availability are just some of the obvious concerns with 5G. And these complicated problems cannot be solved by traditional methods

Solution: Our 5G security team built 5G models in a synthetic simulation environment and identified threat vectors based on industry consortiums (e.g. 3GPP, NSA’s ESF, etc.); MATLAB®’s reinforcement learning tool box was used to expose 5G vulnerabilities and optimize attack patterns based on an objective function. Our 5G security team identified potential mitigation techniques and used the Digital Twin environment to assess their effectiveness.

> **“5G is a critical infrastructure that we must protect from adversarial attacks. It is not sufficient to address known vulnerabilities; instead, we need to leverage reinforcement learning techniques to expose any emerging threat vectors and remediate them. MATLAB®’s Reinforcement Learning toolbox allows us to quickly assess 5G vulnerabilities and identify mitigation methods.”**

Better
- MATLAB®’s simple drag-and-drop GUI interface and feature-rich reinforcement learning toolbox made it easy for our engineers to analyze 5G vulnerabilities, and come up with optimized solutions.

Better Accuracy
- MATLAB®’s Reinforcement Learning toolbox offers metrics for verification and validation purposes. As a result, our RL model achieved a 100% accuracy score

Faster
- Built-in Math and functions libraries to shorten development/analysis time.
- Responsive technical support team to solve issues quickly and professionally

Attribution

LOCKHEED MARTIN

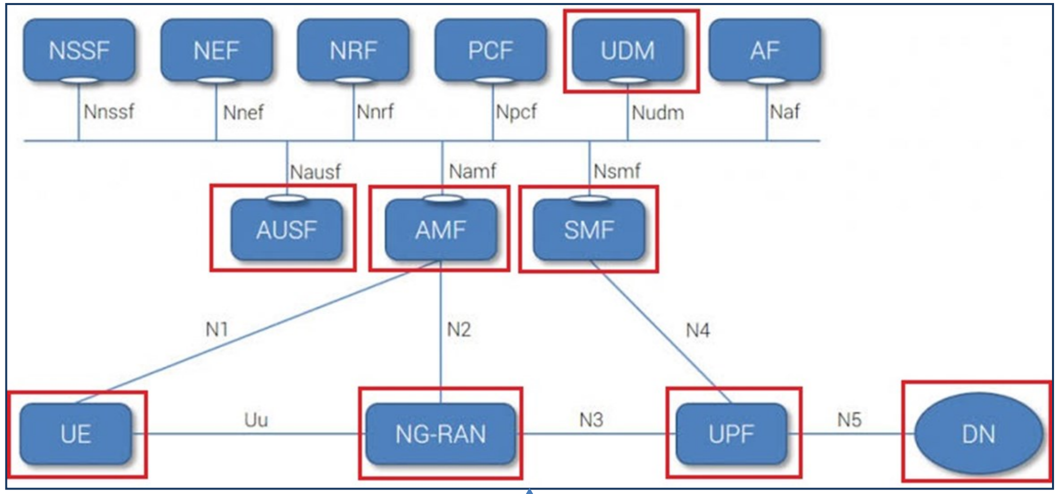
- **EXATA** is a registered **trademark** and brand of Scalable Network Technologies, Inc., Culver City , CA

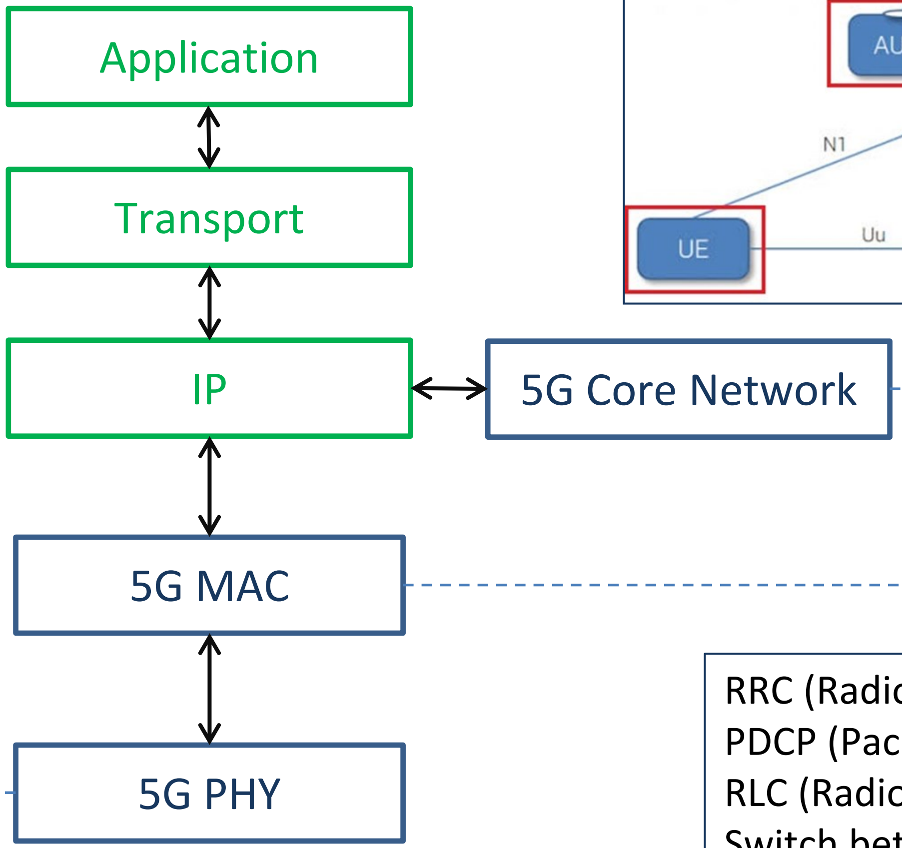
- MATLAB is a registered **trademarks** of The MathWorks, Inc.

LOCKHEED MARTIN

5G MODEL IN EXATA

LOCKHEED MARTIN





Supported

OFDMA/SC-FDMA PHY high-fidelity and high performance model
FDD support for Non-Standalone mode
FDD and TDD support for Standalone mode
FDD and TDD support in FR1 band
TDD support in FR2 band
MIMO channel for multi-antenna operation
Tx/Rx beamforming at gNB in FR2 Band
Numerologies 0,1,2 for TDD/FR1 band
Numerologies 2, 3 for TDD/FR2 band

RRC (Radio Resource Control)
PDCP (Packet Data Convergence Protocol)
RLC (Radio Link Control)
Switch between 5G and Wi-Fi
Carrier Aggregation

Host Vulnerabilities

- A **Host Template** may have multiple vulnerabilities assigned to it
- A **Cyber Attack Template** may have a Cyber Attack Model that exploits a vulnerability
- If a cyber attack template is launched at the host and both the **Host Model** and **Cyber Attack Model** of the templates have matching vulnerabilities, the vulnerability impacts are modeled by EXata

EXATA VULNERABILITY	EFFECT OF VULNERABILITY EXPLOIT
DATABASE_MODIFICATION	Modify data stored in the database server at the victim
DATABASE_SHUTDOWN	Shut down the database server at the victim
DESKTOP_REBOOT	Reboot the victim machine. The victim machine is inactive for the time it takes to reboot (10 seconds)
EMAIL_CLIENT_SHUTDOWN	Shut down the email client at the victim
ENTERPRISE_SERVER_SHUTDOWN	Shut down the specified service at the victim
FILE_MODIFICATION	Read a file stored at the victim (The name of the file is specified by the attacker)
MALWARE_INJECTION	Inject a new malware process at the victim. The malware can propagate to other nodes in the victim's network
NETWORK_INTERFACE_SHUTDOWN	Interface Shut down all network interfaces at the victim
NODE_SHUTDOWN	Shut down the victim node
RESET_ROUTER	Reboot the victim machine. The victim machine is inactive for the time it takes to reboot (10 seconds)
ROUTER_DATA_MODIFICATION	Modify the routing table at the victim
ROUTER_REBOOT	Reboot the victim machine. The victim machine is inactive for the time it takes to reboot (10 seconds)
SQL_INJECTION	Execute an SQL command at the victim
VUL_ACTIONS_WITHOUT_VUL	Send an email; Encrypt all files at the victim node
VUL_DATA_TRANSFER	Transfer data from the victim to the attacker
VUL_DATABASE_CREDENTIALS	Steal database credentials from the victim. This allows the attacker to perform database operations at the victim node
VUL_EMAIL	Read email at the victim node
VUL_EMAIL_CREDENTIALS	Steal email credentials from the victim. This allows the attacker to perform email operations at the victim node
VUL_EXE_ARBITRARY_CODE_VIA_NET	Inject a new malware process at the victim. The malware can propagate to other nodes in the victim's network
VUL_ROOT_CREDENTIALS	Read the specified file stored at the victim; Steal root credentials from the victim. This creates a login shell for the attacker at the victim node with root per missions; Steal credentials for the specified service at the victim; Stop the specified process at the victim node
VUL_ROUTING_TABLE	View Routing Table Reserved for future use
VUL_USER_CREDENTIALS	Install a bot at the victim node
VUL_WEBSERVER	Hack Webpage. Inject a phishing attack at the victim
VUL_WEBSERVER_CREDENTIALS	Steal credentials for the web server from the victim

LOCKHEED MARTIN