Security Analysis for Emerging Cellular Network Technologies

Zizheng Liu, Chunyi Peng

Department of Computer Science, Purdue University

Problem statement

From the specification of 5G emerging technologies, our work tries to detect indications of vulnerability that can be exploited by attacks of the common attack types found in mobile broadband (MBB) network .

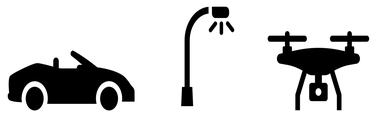
Background

5G mobile broadband (MBB) network is not secure

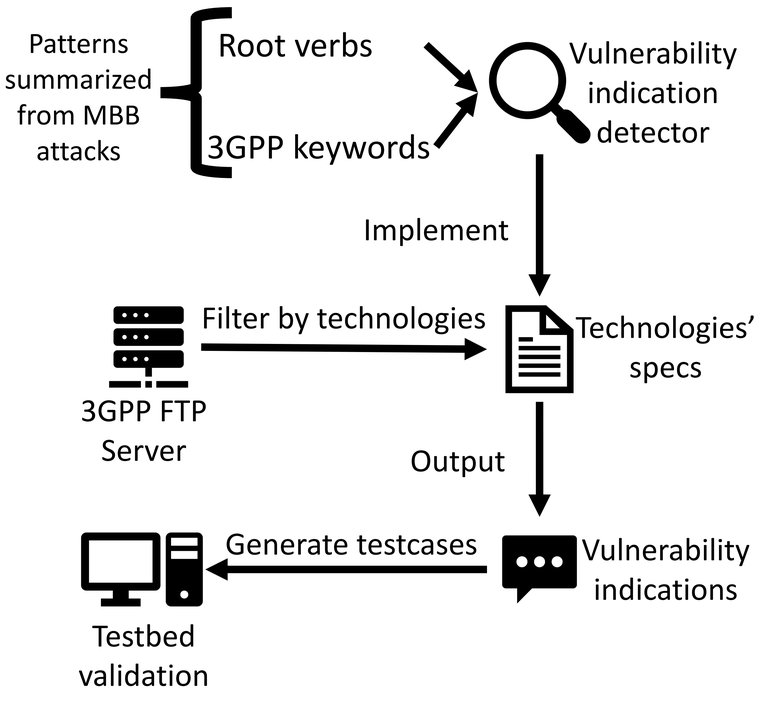
- Eavesdropping attacks
- Downgrade attacks
- DoS attacks

5G network also supports other technologies

- Cellular V2X
- Cellular IoT
- UAS over 5G



Methodology



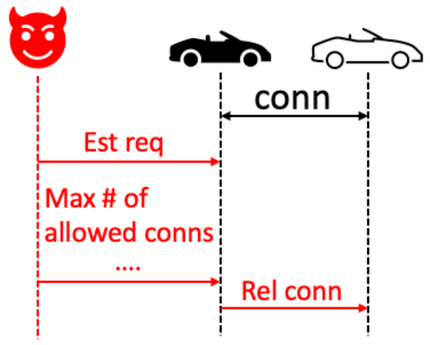
Summarized patterns and implementation results

Attack type	Root verbs	3GPP keywords	Impl results	C-V2X	UAS over 5G	CIoT
Eavesdropping & Downgrade	contain	'id', 'capacity', 'security'		39	23	5
DoS	initiate/exchange	'release', 'reject'		49	5	6
	not + initiate/exchange	'establish ment'		6	6	1

Showcase attacks

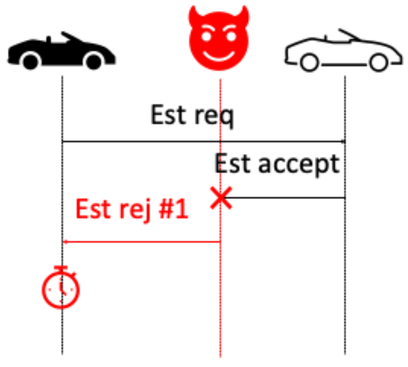
"The initiating UE may initiate the procedure to release an established PC5 unicast link if the UE has reached the maximum number of established PC5 unicast links and there is a need to establish a new PC5 unicast link."

Vulnerability indication from TS24.587



"If the PC5 signalling protocol cause value in the DIRECT LINK ESTABLISHMENT _REJECT message is #1 "direct communication to the target UE not allowed" or #5 "lack of resources for PC5 unicast link", then the UE shall not attempt to start the PC5 unicast link establishment procedure with the same target UE at least for a time period T."

Vulnerability indication from TS24.587



Contribution to thrust 4: AI-Powered Network Security

In this work, we design a security analysis framework leveraging NLP techniques and 3GPP domain knowledge to detect vulnerabilities of emerging cellular network technologies from their specifications.

Plan for collaboration with other thrust

- Collaboration with thrust 8 (Security and Privacy of Network Users)
  - Technologies analyzed in our work are the most common scenarios where distributed learning is used.
  - Vulnerabilities found in our work help researchers in thrust 8 to design more secure and private communication mechanisms for distributed systems.

Contribution to use cases

Use Case 2: This work can be used for security analysis of different technologies with mobility protocols.
Use Case 3: The security issues discovered in this work can be used to guide the design of future cellular networks with higher security requirements.

Acknowledgements

This material is based upon work supported in part by National Science Foundation under award ID IIS-2112471.