Zero Trust Chain (ZTC): Security Solutions for 5G Networks with an O-RAN-Centric and Device-Centric Approach

Yongkyu Jang, Dr. David J. Love, Dr. Christopher G. Britton, Dr. Sonia Fahmy, Dr. Remi Chou, Dr. Vuk Marojevic, Dr. Syed Rafaal Hussain, Dr. Hyuck Kwon, Dr. Sang W. Kim, Dr. Taejoon Kim

1 Purdue University, 2 The University of Texas at Arlington, 3 Mississippi State University, 4 The Pennsylvania State University, 5 Wichita State University, 6 Iowa State University, 7 The University of Kansas

ABSTRACT

- Our team, named Zero Trust X (ZTX), proposes a software solution that enables military squads to securely share situational awareness in their operations through high-performance, but often untrusted, 5G networks.
- It will allow DoD operators to discover malicious entities in near-real-time and provide communication mechanisms to avoid adversary’s control over DoD traffic.
- Specifically, through a minimum amount of cooperation with the network operator, part of our solution leverages O-RAN for new threat monitoring and mitigation solutions specifically designed for 5G networks.
- We complement this O-RAN-centric approach with a device-centric approach to ensure that DoD devices also implement their own layer of security.
- Such a combination will substantially enhance the security of the whole system.

Device-Centric Threat Monitoring/Mitigation

Real Time Anomaly Detection & Secure Slicing

O-RAN & Core-Centric Threat Monitoring/Mitigation

Waveform-Level Intrusion Detection (Fig. 1.a)
- RNN-based solution has a detection performance that improves with increased signal observation length and network depth.
- Two-stage, hierarchical RNN intrusion detection method:
  - Stage 1: Intrusion detection. Low-complexity, direct UE implementation that enables near-Real Time intrusion detection with small power consumption. (Single layer RNN)
  - Stage 2: A higher-complexity, multi-layer RNN executed on the UEs for categorizing the threat.

Control Plane Threat Detection (Fig. 1.b)
- 5GThreatDetector have two main components:
  - (1) An automatic signature synthesizer for capturing attacks.
  - (2) A runtime-monitor for monitoring the device’s cellular network traffic for those behavioral signatures and taking corrective measures based on its deployment.

Adaptive Double-Layer Encryption

What is Double Layer Encryption (DLE)? DLE is the outer layer encryption done by the customer at his UE application layer, whereas the inner layer encryption is any other encryption done/installed/operated by a phone manufacturer, system operator, or anyone else.

How it works?:
- Encryption key is selected by the customer (i.e., TX), and shared with the RX in prior to communications.
- The DLE software is installed by the customer himself at his phone application layer.
- The DLE key is the one-time password and can be delivered to a user through several channels.

How to check integrity at RX?: Ex appends a tag \( T = h(K, M) \) to the message \( M \), where \( K \) is the shared secret key between Tx and Rx, and \( h \) is a hash function. Compared to network-based detection schemes, this approach does not require data collection and analysis from multiple UEs and gNBs. Therefore, the network protocol overhead, implementation complexity, and detection latency can be significantly reduced.

Security Challenge: 5G systems do not have any extra layer for secret message transfer.
- Error permeates to the application layer when CRC-misdetection happens.

ZTX solution: An extra error correcting layer + coderow distribution adaptation using secret encoding/decoding.
- The stealth communication block combines these error correcting blocks with secret message encoder/decoder.

ACKNOWLEDGEMENT This work is supported by the National Science Foundation (NSF) under Grant 1TE2226447 and ITe2326898, as part of the NSF Convergence Accelerator Track G: Combating Vulnerability and Unawareness in 5G Network Security.