

STRIDEtastic(0): Research Introduction

Francisco Wulf

Pontificia Universidad Católica de Chile

francisco.wulf@uc.cl

Abstract—This document presents the first increment on the investigation "STRIDEtastic: Threat Modeling and Security Evaluation of Meshtastic Networks through Practical and Theoretical Attacks". It discusses introductory information for the investigation, namely: context, motivation, research goals, questions, hypothesis, scope, limitations and methodology overview.

I. INTRODUCTION

A. Context and Motivation

In recent years, the Meshtastic project has gained significant traction as an off-grid communication protocol built upon LoRa (Long Range) radio interfaces. It is designed to create decentralized mesh networks, enabling peer-to-peer communication without relying on existing telecommunications infrastructure. This makes Meshtastic particularly valuable in contexts where conventional networks are unavailable or unreliable, such as during natural disasters or in conflict zones. Meshtastic has seen increased adoption in Europe, with robust networks forming in countries like the United Kingdom and Spain, and is now gaining momentum in Latin America, notably in Argentina and Chile.

While Meshtastic offers resilience and independence from centralized systems, its increasing use in critical scenarios also raises pressing concerns around security. In emergency or wartime conditions, secure communications are paramount. Though the Meshtastic application includes certain security features, the underlying architecture remains susceptible to a range of attacks. This research is motivated by the need to assess the current state of security in Meshtastic and contribute to its development through constructive security analysis.

B. Research Objectives

The primary objectives of this research are:

- Assess the current security implementation of Meshtastic networks.
- Identify and replicate known vulnerabilities in a controlled lab environment.
- Build a STRIDE-based threat model for doing threat analysis.
- Raise awareness about potential risks within the Meshtastic ecosystem.
- Provide insights and propose mitigation that could guide developers toward implementing more secure communication models, while staying within the protocol's inherent constraints.

C. Research Questions

This research is guided by a set of investigative questions that aim to structure the security evaluation of Meshtastic and uncover weaknesses both theoretically and practically. The STRIDE threat model (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) is used where appropriate to frame the threat analysis.

- 1) **RQ1:** To what extent does Meshtastic provide security guarantees across everyday use cases and semi-industrial applications?
- 2) **RQ2:** What security mechanisms are currently implemented in Meshtastic, and how well do they mitigate threats categorized under STRIDE?
- 3) **RQ3:** Which known vulnerabilities and attack scenarios can be replicated in a controlled environment?

D. Hypothesis

These research questions establish the foundation for a critical evaluation of the Meshtastic protocol. Based on existing documentation, prior vulnerabilities in similar technologies, and initial observations, we hypothesize the following:

While Meshtastic integrates basic cryptographic protections and attempts to ensure secure communication, the protocol remains vulnerable to a variety of attacks. These are not necessarily related to encryption weaknesses but rather stem from protocol-level or implementation-level assumptions and flaws. Adversaries may be capable of combining known attacks in novel ways to compromise network integrity, confidentiality, or availability.

E. Scope and Limitations

This research is scoped as a high-level and partially low-level security evaluation of the Meshtastic (v2.7.3) communication and routing protocols. It focuses on analyzing known attack vectors (such as spoofing, sniffing, tampering, etc.) and explores how these can be intelligently combined to amplify their impact. The research does **not** aim to identify or disclose zero-day vulnerabilities or conduct a full reverse engineering of firmware. The analysis is limited to simulated environments with real devices.

F. Methodology Overview

The methodology consists of the following steps:

- 1) Review existing Meshtastic protocol documentation and community discussions.
- 2) Identify and catalog known vulnerabilities and attack patterns relevant to Meshtastic.

- 3) Structure the security analysis using the STRIDE threat modeling framework to classify potential risks (e.g., spoofing, tampering, denial of service).
- 4) Design and implement a series of lab experiments to reproduce selected attacks in a private, controlled testbed.
- 5) Evaluate the potential impact of these attacks on confidentiality, integrity, and availability.
- 6) Discuss mitigation strategies and propose recommendations to enhance security without imposing unsustainable overhead on the protocol.