CONCORDIA INSTITUTE FOR INFORMATION SYSTEM ENGINEERING (CIISE)
CONCORDIA UNIVERSITY

INSE 6120
CRYPTOGRAPHIC PROTOCOLS AND NETWORK SECURITY

WINTER 2024

SECURITY ASSESSMENT OF THE TETRA PROTOCOL

Submitted to:

Prof. Ivan Pustogarov

By:

Student ID	Name
40262702	Zohre Farzaneh Kaloorazi
40225369	Divine Anyalemechi
40235545	Adithya Ananth
40273656	Oghenerukevwe Oyinloye
40242392	Seth Ekow Abaidoo
40174534	Azeez Ogede
40278569	Vaishnavi Naikwade

January 30, 2024

INTRODUCTION

Tetra burst is a radio protocol designed with four different encryption algorithms. The cryptographic primitives used by Tetra are all stream ciphers. These encryption algorithms are allocated to different countries. These Protocols are allocated such that -TEA1 (is used by majority countries including not to export countries of the EU), TEA2 (reserved for the military), TEA3 (countries the European Union have some relations), TEA4 (no information is given on it hence it is assumed that it isn't in current use).

Research has revealed that there are five key vulnerabilities that they observed by reverse engineering carried out by the and midnight blue (2023) and Zahednejad et al.,2020 who had earlier mentioned one vulnerability (CVE-2022-24400) in the established vulnerabilities by midnight blue.

PROPOSED PROJECT STRUCTURE

The team 1 will be working on the security assessment of the Tetra Protocol following these subheadings:

1. Why tetra protocol- The focus is to determine the purpose of the protocol
2. What is the protocol- The subsystem of the protocol and techniques used to actualize the protocol, the cryptographic primitives used by the system and attempt to preempt how they interoperate.
3. How the protocol works- where the protocol has been implemented across different sectors and attempt to determine the abstract model of the protocol that has been broken TEA1.
4. Vulnerabilities that have been established based on research reviews from 2020 to 2024.
5. Analyze Risks and Determination of the Potential Impact of the reported vulnerabilities; - based on
    a. devices, the data and network traffic where it has been deployed,
    b. the level of cryptanalysis and attack that can be done on transmitted data,
    c. potential risk- which will be based on these factors-
        i. Ease of exploitability
        ii. Discoverability of the security weakness

iii. Reproducibility of threats (some threats are one-time and some are continuous)

iv. Prevalence of the threat in the industry or similar companies

v. Historical security incidents