TETRA security disclosures

Introduction

In August 2023, a group of security researchers published papers describing a set of findings relating to TETRA security. TCCA has prepared this document to describe the impact of these findings and possible mitigations.

Background

Researchers working for security consultancy Midnight Blue were funded by the NLnet Foundation, which financially supports organisations and people that contribute to an open information society, to conduct research into TETRA security. The researchers reviewed the open TETRA standards published by ETSI, and reverse engineered publicly available equipment to recover algorithms that are only available under confidentiality agreements.

Following a responsible disclosure process, early research findings were disclosed in strict confidence to ETSI in January 2022 to enable mitigations to be made in TETRA security standards before the research was published. ETSI TCCE was already working on an additional set of algorithms for a next release of the TETRA standard to maintain TETRA security into the 2040s, and so additional mitigations were added into the ongoing standardisation work. Revised TETRA security standards were published in October 2022, and TETRA manufacturers and suppliers already have software upgrades available that address some of the findings.

The research findings were made public by Midnight Blue in August 2023 at Black Hat USA, and subsequent security conferences.

Findings on the TEA1 encryption algorithm

The researchers' findings all apply to air interface encrypted systems. Clear systems are not affected. There are no findings that affect authentication. End-to-end encryption was not examined in the research, and generally uses well known public domain algorithms such as AES128 or AES256, or government owned algorithms.

The main finding, raising most concerns in the user community, is about the TEA1 encryption algorithm which internally reduces the effective length of the encryption key, thus requiring less effort than expected to recover the reduced key and decrypt communications.

No issues were found with the TEA2 algorithm, and it is considered to be safe for continued use. The researchers noted an anomaly in a table in the TEA3 algorithm. However, independent reviewers do not believe that this leads to any weakness in TEA3 in the way that it is used in TETRA, and TEA3 is also considered to be safe.

TCCA, Unit 14, Baker's Yard, Christon Road
Gosforth, Newcastle Upon Tyne NE3 1XD, UK
T +44 (0) 191 231 4328 E admin@tcca.info

TEA1 was conceived in the mid-1990s to be easily exportable. The key reduction was therefore needed to comply with the Wassenaar Arrangement[1] signed by many countries – 42 at present – limiting the exports of military and 'dual use' (military and civilian applications) technologies, which includes cryptography. In the TEA1 algorithm design, the key length was reduced to an equivalent of 32 bits to permit worldwide export according to the Arrangement. The actual value of the equivalent key length had not been public before the Midnight Blue publication, but the status of TEA1 as an export-friendly variant was public.

TETRA algorithms are currently available only to suppliers under a strict non-disclosure agreement, and so the design of the TEA1 algorithm had to be kept secret by manufacturers and remained as such until the research findings were published. Although many encryption systems today are fully published to allow open scrutiny and research, when TETRA was designed it was far more normal to keep algorithms secret – especially for security systems that protect government communications. Part of the security of TEA1 was provided by the secrecy of the algorithm.

Mitigation

End-to-end encryption can be used to protect speech and/or data and is not affected by any attack on TEA1. An alternative algorithm, either TEA2 or TEA3 from the original set, or TEA5, TEA6 or TEA7 from the additional algorithm set introduced in 2022, can be used in place of TEA1 to protect speech, data and signalling. TEA2 and TEA3 use 80 bit keys without any reduction in the key length, but deployment of these algorithms is more restricted than TEA1. The new algorithms TEA5 and TEA6 use 192 bit keys without any reduction but are also restricted in where they can be deployed. The new algorithm TEA7 has an effective key length reduction to 56 bits and will be available in many countries as per the Wassenaar Arrangement.

Other findings

The research also found a weakness of the identity encryption that could allow an attacker to discover the numerical identities (SSIs) of the users (not the personal identities of the users themselves). Direct Mode Operation (DMO) uses a different mechanism and is not vulnerable to this attack.

The additional encryption algorithms, TEA5, TEA6 and TEA7 have been designed together with a different authentication and key management algorithm set TAA2 which uses a different identity encryption process which is not vulnerable to the attack. Migration to TAA2 would completely solve the issue. TAA2 is implemented when migrating to TEA5, TEA6 or TEA7.

Finally, the research also contained two secondary findings, which can be solved by a software upgrade of mobile stations. Despite the low probability of either attack being carried out in a real system environment, changes have been made in the TETRA standard to mitigate these findings and these are no longer considered to be an issue.

Recommended actions

Any TETRA system operator or user should work with their national cybersecurity agencies and with their suppliers to assess whether the findings provide a material risk to their system operation. This will depend on their specific threats and threat actors, and the consequences of the threats being acted upon.

[1] *https://www.wassenaar.org/*

The findings that are not related to algorithms only require a software update to completely mitigate, and some suppliers already have updates available. Transition to a new algorithm is complex, and system operators should consult their suppliers to investigate implications and timescales.

TCCA Working Groups have already input significantly on addressing these issues, and further information is available to TCCA members here (log in required).

ETSI TCCE will make the primitives of all TETRA Air Interface cryptographic algorithms* available as part of the TETRA documentation set but will maintain the requirement for a CRUU and confidential handling of the full set of documentation applying to such algorithms.

*In this case the primitives of the algorithms relate to the algorithm specification and not any example code or test data.

For more information on the security issues in this paper, please contact david.chater-lea@tcca.info

On behalf of its members, TCCA supports all standard mobile critical communications technologies and complementary applications. Our members are drawn from end users, operators and industry across the globe. We believe in and promote the principle of open and competitive markets worldwide through the use of open standards and harmonised spectrum.

For more information on TCCA, please contact admin@tcca.info

If you want to help shape the future of critical communications – Join us!