EXPLOIITM

eCTF10 — 10 YEARS OF THE EMBEDDED CAPTURE THE FLAG

Indian Institute of Technology, Madras

Abhinav I S, Arivoli R, Athish Pranav D, Kevin Kinsey, Madhav Tadepalli, Md Isfarul Haque, Mohit M B, Nithin Ken Maran, Nitin G, Sanjeev Subrahmaniyan

Advised by: Dr. Chester Rebeiro

January 16, 2025 - April 16, 2025

Design Overview

Secure Access Control: Subscriptions are unique to specific decoder IDs, channels, and time ranges, with both subscriptions and frames encrypted via AES-CBC using decoder-ID and timestamp-specific keys, with randomized IVs, and HMAC authentication.

Robust Attack Resistance: Rust-based decoder and HAL for memory safety, with constant-time comparisons, SHA-3 hashes, and safety bit set in flash, with a lockdown period to prevent brute-force attempts.

Tamper-Resistance: Only encrypted subscriptions are stored in flash, preventing in-place modification or unauthorized access.

Security Requirements

No subscription? No TV	Finders are not keepers	Time's always ticking
Broadcast frames are encrypted with timestamp-specific keys and can be decrypted only with valid subscriptions.	**Subscription updates are encrypted using a key derived solely from the target decoder ID.**	**Replay attacks are mitigated by maintaining a record of the latest timestamp across all channels.**

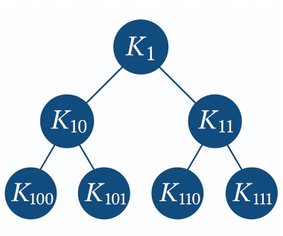
Defensive Highlights

Per-timestamp Keying:

Enhanced security is achieved by assigning a **unique key to each timestamp.**

The segment-tree **compresses key sets**, avoiding storage of each individual key.[1]

Key Distribution and Derivation:



Subscription updates provide the **necessary data to derive keys for valid timestamps.**

Keys are derived using hashing of roots with salts for left and right leaves.

Restricted Access, by design:

This structure enforces **downward-only traversal.**

It is **impossible to derive keys for unauthorized timestamps.**

Digital Signature:

Tampering with the content of subscription updates and frames is **securely prevented.**

Provides protection against CPA analysis on HMAC computations[3].

Offensive Highlights

IV Manipulation:

Manipulate IV of AES-CBC-encrypted frames **with no IV authentication**, to manipulate underlying plaintext.

Replay Attack:

Pass **identical frames** on emergency channel, and out-of-order timestamps across different channels to exploit improper implementation of timestamp progression.

Oracle Attacks:

Exploit padding and **decryption oracle** vulnerabilities in poorly secured implementations to **recover plaintext** from ciphertexts.

RAM Dump Exploits:

Exploit buffer overread vulnerabilities to perform memory dumps and **extract sensitive data** such as keys and secrets.

Voltage Glitching:

Inject glitches to bypass security checks by **forcing authentication functions to return false positives**.[2]

References

1. https://drive.google.com/file/d/1vT8omy96u64AmXFzBeddBlFwNUD2NuLK/view
2. https://www.newae.com/chipwhisperer
3. https://link.springer.com/content/pdf/10.1007/978-3-030-89915-8_2.pdf