EM Analysis in the IoT Context: Lessons Learned from an Attack on Thread

Daniel Dinu[1], Ilya Kizhvatov[2]

[1]Virginia Tech

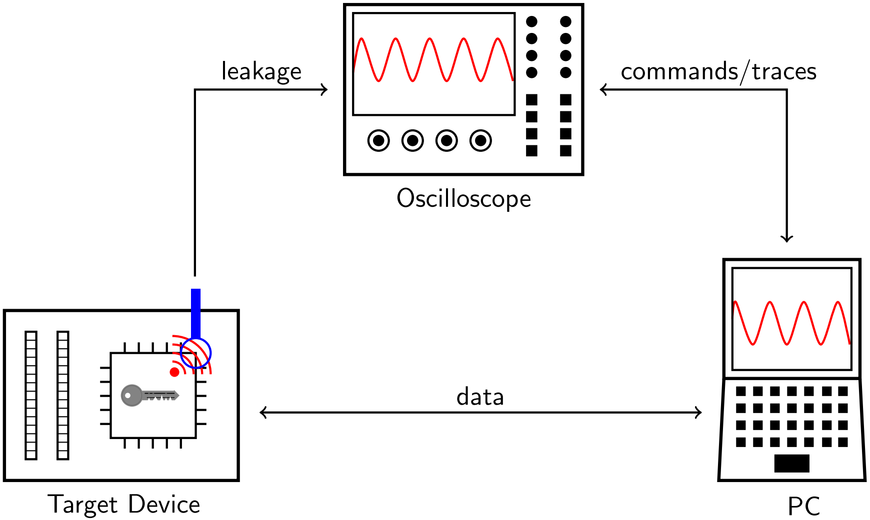
[2]Radboud University Nijmegen

CHES 2018

Radboud University Nijmegen

Outline

EM Analysis


leakage
commands/traces
Oscilloscope
data
Target Device
PC

Thread

- Networking protocol for the IoT
- Simple for consumer
- Built-in security
- Power efficient
- IPv6 connectivity
- Robust mesh network
- Runs on IEEE 802.15.4 radio silicon

More than 100 members

Motivation

- Numerous low-cost hardware and software tools for side-channel attacks
- Evaluate the effort required to apply an EM attack in the IoT context

Do cryptographic implementations in the network layer need protection against side-channel attacks?

Outline

Communication Security

- Security is enforced at two layers:
  - Medium Access Control (MAC) — AES–CCM using key K_{MAC}
  - Mesh Link Establishment (MLE) — AES–CCM using key K_{MLE}

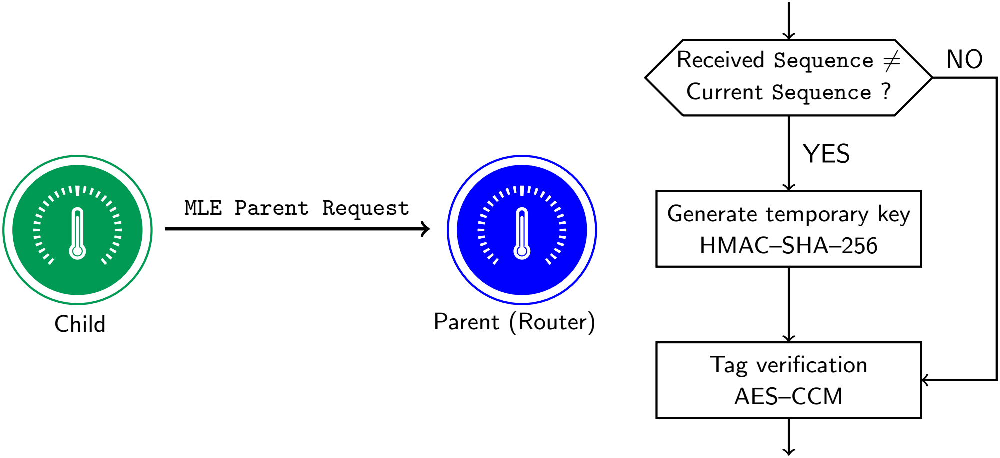
- A node gets the master key K when it is commissioned to a Thread network

- Fresh keys are generated from the 16-byte K and 4-byte `Sequence` number:

$$K_{MAC} \mathbin{||} K_{MLE} = \mathit{HMAC\text{–}SHA\text{–}}256(K, \texttt{Sequence} \mathbin{||} \text{“}\mathit{Thread}\text{”})$$

- The default key rotation period is set to 28 days

Processing a `MLE Parent Request` Message



AES–CCM

- Combines CBC–MAC mode and CTR mode
- The execution of both modes of operation can be attacked
- The attacker can control up to 12 input bytes of the first block:
  - `Source MAC Address` – 8 bytes
  - `Frame Counter` – 4 bytes
- Known attack: Jaffe [CHES'07], O'Flynn and Chen [COSADE'16]

AES-CBC	49	`Source MAC Address`	`Frame Counter`	05	00	15
AES-CTR	01	`Source MAC Address`	`Frame Counter`	05	00	01

Relationship between K and K_{MLE}

Master key to MLE key ($K \longrightarrow K_{MLE}$)

- Key derivation using HMAC

Relationship between K and K_{MLE}

Master key to MLE key ($K \longrightarrow K_{MLE}$)

- Key derivation using HMAC

MLE key to master key ($K_{MLE} \longrightarrow K$)

- Send `MLE Child ID Request` to ask for the master key
- The `MLE Child ID Response` includes the master key

Relationship between K and K_{MLE}

Master key to MLE key ($K \longrightarrow K_{MLE}$)

- Key derivation using HMAC

MLE key to master key ($K_{MLE} \longrightarrow K$)

- Send `MLE Child ID Request` to ask for the master key
- The `MLE Child ID Response` includes the master key

Master key and MLE key are equivalent!

$$K \longleftrightarrow K_{MLE}$$

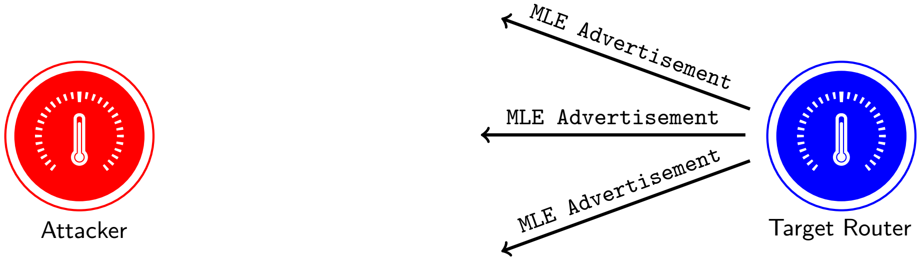
Outline

The Most Feasible Attack

Attacker

Target Router

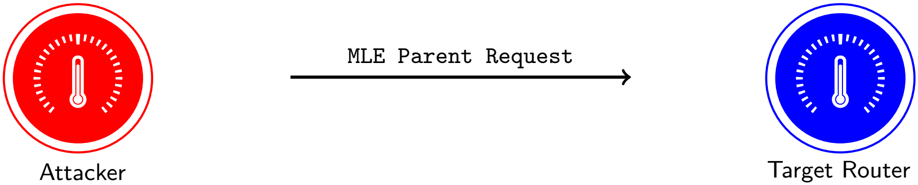
The Most Feasible Attack



Step 1: Observe an `MLE Advertisement` message

- Record the `Sequence` number

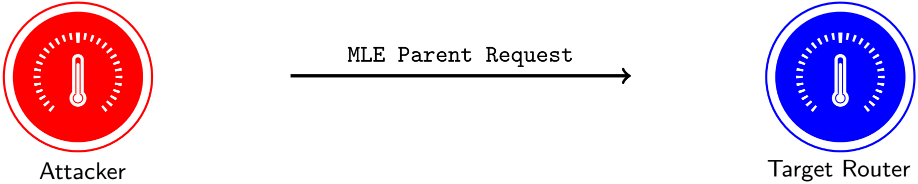
The Most Feasible Attack



Step 2: Inject `MLE Parent Request` messages

- Recorded `Sequence` number
- Random `Source MAC Address` and `Frame Number`

The Most Feasible Attack



Step 3: Observe the EM leakage

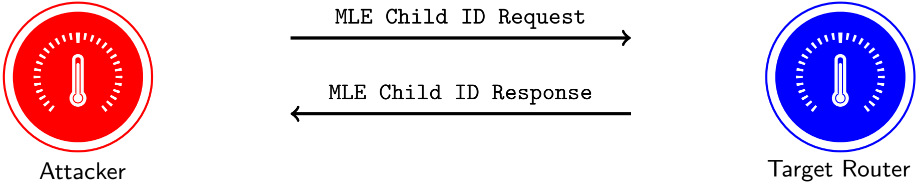
- Save the injected inputs and corresponding EM traces

The Most Feasible Attack

Step 4: Recover the MLE key K_{MLE}

- Mount a DEMA attack

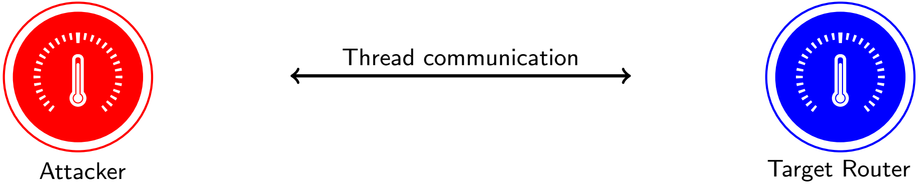
The Most Feasible Attack



Step 5: Get the master key K

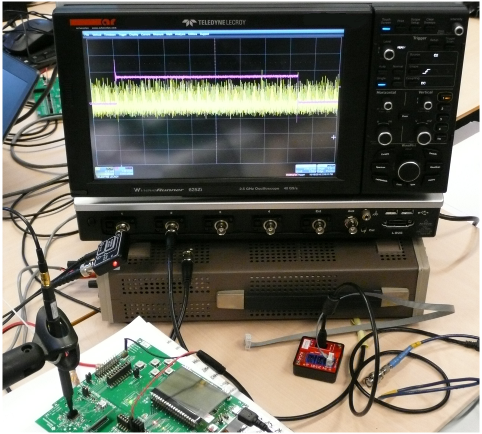
- Send a `MLE Child ID Request` message
- The `MLE Child ID Response` message contains K

The Most Feasible Attack



Full network access!

Experimental Setup



- Target: TI CC2538 (Cortex-M3, 32 MHz)
- Thread stack: OpenThread
- Oscilloscope: LeCroy waveRunner 625Zi
- Langer EM probes
- No trigger signal from target!

Results

- Sampling rate set to 1 GS/s
- 10,000 EM traces acquired in about 3 hours
- Full recovery of the MLE key K_{MLE}
- Two key bytes were much more difficult to recover than the rest
- Message fragmentation prevented recovery of the master key
- The attack may succeed on other implementations of the stack

Outline

Countermeasures

- Shielding & tamper resistance
- Protected cryptographic implementations
- Protocol level mitigations
- Security certification scheme

Countermeasures

- Shielding & tamper resistance
- Protected cryptographic implementations
- Protocol level mitigations
- Security certification scheme

A combination of the above countermeasures
is recommended for high security!

Outline

Lessons Learned

Lessons learned from our evaluation
can be applied to other IoT systems and protocols.

Lessons Learned

Lessons learned from our evaluation
can be applied to other IoT systems and protocols.

- Prevent electromagnetic leakage

Lessons Learned

Lessons learned from our evaluation
can be applied to other IoT systems and protocols.

- Prevent electromagnetic leakage
- Do not allow access to the master key from temporary key(s)

Lessons Learned

Lessons learned from our evaluation
can be applied to other IoT systems and protocols.

- Prevent electromagnetic leakage
- Do not allow access to the master key from temporary key(s)
- A network-wide master key is a double-edged sword

Lessons Learned

Lessons learned from our evaluation
can be applied to other IoT systems and protocols.

- Prevent electromagnetic leakage
- Do not allow access to the master key from temporary key(s)
- A network-wide master key is a double-edged sword

Side-channel attacks are a real threat for the IoT!


SECURE

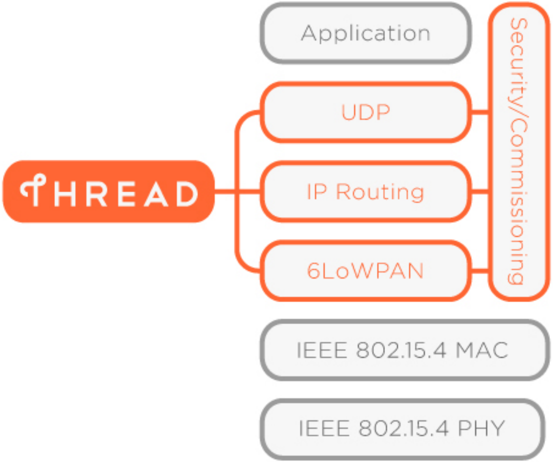
Thank you!

Appendix

References

- Joshua Jaffe. *A first-order DPA attack against AES in counter mode with unknown initial counter*. In Cryptographic Hardware and Embedded Systems - CHES 2007.
- Colin O'Flynn and Zhizhang Chen. *Power analysis attacks against IEEE 802.15.4 nodes*. In Constructive Side-Channel Analysis and Secure Design - COSADE 2016.

Thread Stack

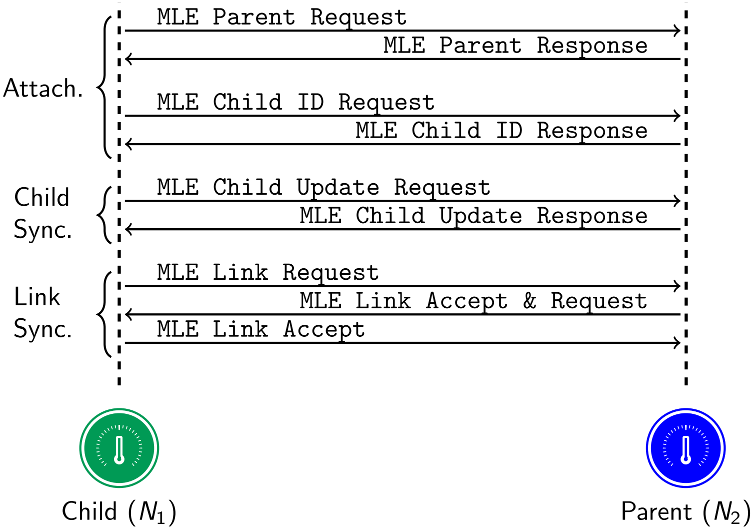


Source: https://www.threadgroup.org/

Mesh Link Establishment (MLE)

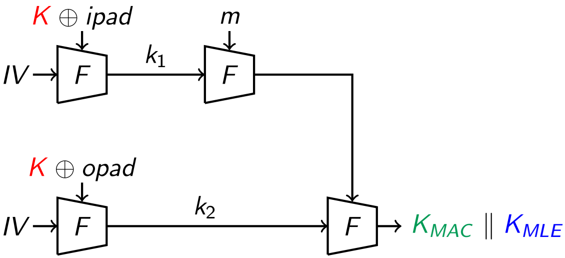
- Facilitates the secure configuration of radio links
- Allows exchange of network parameters
- MLE messages are sent inside UDP datagrams
- Routers periodically multicast `MLE Advertisement` messages
- Link configuration is initiated by a `MLE Parent Request` message

Establishing a Communication Link



HMAC–SHA–256

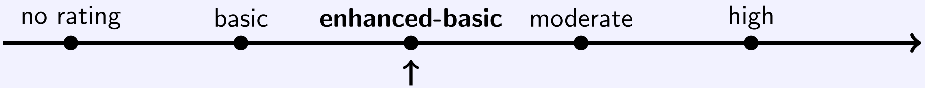
- $m = \texttt{Sequence} \parallel \text{“}\mathit{Thread}\text{”} \parallel \texttt{0x80 0x00} \ldots \texttt{ 0x00} \parallel \mathit{len}$
- The attacker targets k_1 and k_2
- k_1, k_2, and Sequence give K_{MAC} and K_{MLE}
- Not enough control of the input!



Attack Feasibility

Attack Effort

- Adaptation of the rating for smart cards from the Joint Interpretation Library
- Last step of the attack is feasible ⇒ **enhanced-basic**



Equipment Cost

Cost	Oscilloscope	Attack Success
HIGH	**LeCroy WaveRunner 6Zi**	✓
MEDIUM	PicoScope, ChipWhisperer-Pro	✓
LOW	ChipWhisperer-Lite	✗

Guessing Entropy

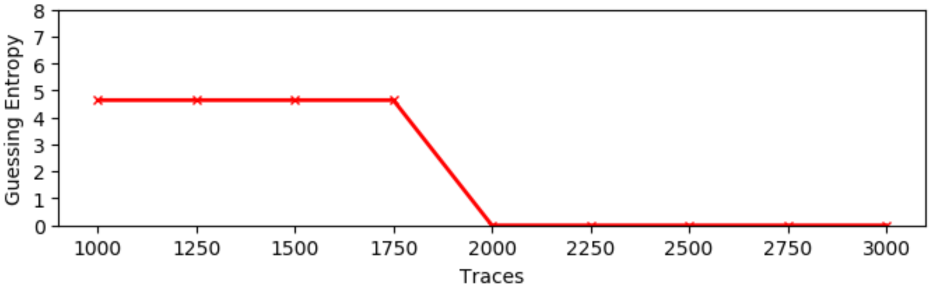


Figure: Evolution of the guessing entropy for the second key byte.

Correlation Matrix

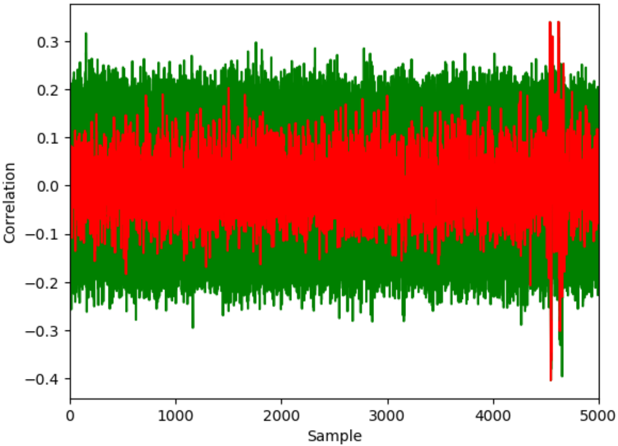


Figure: Correlation of all key candidates for the second key byte when using 3,000 traces.