Internet of Things

Lecture 8 - Standardized Security Solutions for IoT

Main Challenges

- Very large attack surface and widespread deployment
- Limited device resources
- Security by design not a top priority
- Lack of expertise
- Applying security updates

Security Requirements

- Well-known CIA security model
- Confidentiality
  - ensure that only the intended receiver can read/interpret a message
  - unauthorized access is prevented
- Integrity
  - ensure that a message cannot be modified
  - unauthorized individuals should not be able to destroy/alter message
- Availability
  - ensure that system/network is able to perform its tasks without interruption
  - often measured in terms of percentages of up/down time

IoT Stack - Security Solutions

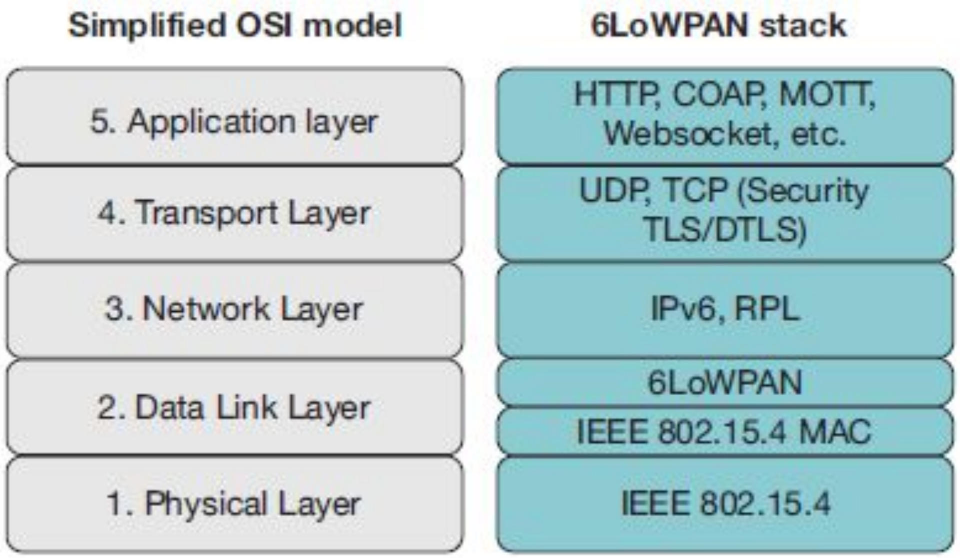


Table 1: IoT stack with standardized security solutions.

IoT Layer	IoT Protocol	Security Protocol	Scope
Application	CoAP, HTTP	User-defined	E2E
Transport	UDP, TCP	DTLS, TLS	E2E
Network	IP	IPsec	E2E
Routing	RPL	RPL security	Per-hop
6LoWPAN	6LoWPAN	None	None
Data-link	IEEE 802.15.4	802.15.4 security	Per-hop

IEEE 802.15.4

Security Level/Id	Security Suite	Confidentiality	Integrity
000	None	✗	✗
001	AES-CBC-MAC-32	✗	✓
010	AES-CBC-MAC-64	✗	✓
011	AES-CBC-MAC-128	✗	✓
100	AES-CTR	✓	✗
101	AES-CCM-32	✓	✓
110	AES-CCM-64	✓	✓
111	AES-CCM-128	✓	✓

Source: M Shila, Devu & Cao, Xianghui & Cheng, Yu & Yang, Zequ & Zhou, Yang & Chen, Jiming. (2014). Ghost-in-the-Wireless: Energy Depletion Attack on ZigBee.

IEEE 802.15.4 - Data integrity & confidentiality

- Data integrity
  - MAC (aka MIC)
  - Hash function over the message and pre-shared secret key
  - Receiver recomputes and verifies MAC
  - AES-CBC-MAC and AES-CCM with 3 MAC lengths
- Data confidentiality
  - Encryption
  - Semantic security using a nonce
  - Differentiate between similar or identical messages
  - 13 bytes nonce
  - Source address (8 bytes) + frame counter (4 bytes) + security control field (1 byte)

IEEE 802.15.4 - Replay Protection & Access Control

- Replay Protection
  - Increasing frame counter
  - Receiver rejects msgs with smaller sequence numbers
  - 32 bits counter
  - Part of nounces
- Access Control
  - Access control list (ACL)
  - Verify source address of packets
  - Bypassed by spoofing attacks

RPL

- Several security mechanisms against routing attacks
- Secure RPL routing packets
- Security Section to the RPL header -> security type
- 3 security modes:
    - unsecured - no security
    - preinstalled - keys are preinstalled on nodes
    - authenticated - nodes receive keys from key authority after authentication

RPL

- Security Services
  - data confidentiality
  - data authenticity
  - replay protection
- AES-128 CCM - encryption & MAC
- RSA with SHA-256 - signature
- AES-128 CCM nonce
- Key Identifier Mode (KIM), Security Level (LVL)
- Consistency Check (CC)

	KIM=0,1,2	
LVL	Attributes	MAC Len
0	MAC-32	4
1	ENC-MAC-32	4
2	MAC-64	8
3	ENC-MAC-64	8
4-7	Unassigned	N/A

	KIM=3	
LVL	Attributes	Sig Len
0	Sign-3072	384
1	ENC-Sign-3072	384
2	Sign-2048	256
3	ENC-Sign-2048	256
4-7	Unassigned	N/A

CoAPs (CoAP + DTLS)

- DTLS - transport layer security
  - data confidentiality and integrity, authentication
  - non-repudiation, anti-replay protection
- CoAP with DTLS support => CoAPs
- Provisioning phase
  - Device identifiers are collected and stored on server
  - Identifiers list => access control list (ACL)
  - Devices receive keys and ACL

CoAPs (CoAP + DTLS)

- 4 security modes: NoSec, PreSharedKey, RawPublicKey, Certificates
- PreSharedKey
  - pre-programmed with symmetric shared keys
  - list of shared keys
  - TLS_PSK_WITH_AES_128_CCM_8 cipher suite
- RawPublicKey
  - pre-programmed with asymmetric key pair
  - TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 cipher suite

CoAPs (CoAP + DTLS)

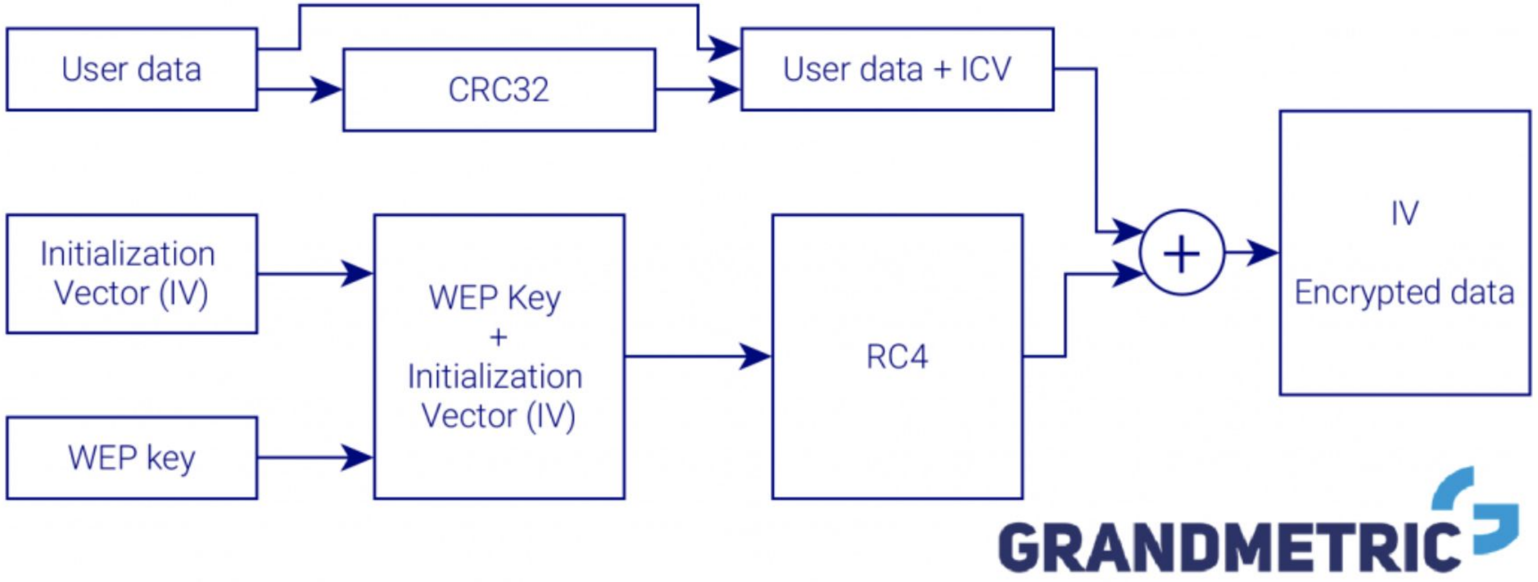
- Certificates
  - Asymmetric keys
  - X.509 certificate
  - List of trust anchors
  - Signature generated using ECDSA and SHA-256
  - TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 cipher suite
  - Device authentication using ECDSA
  - Key agreement using ECDHE
- ECC used in 2 security modes
  - strong security, small keys, less processing power

Wi-Fi

- More and more used
- Security protocols: WEP, WPA, WPA2, WPA3
- Krack attack for WPA2
  - replay attack
  - vulnerability in the 4-way handshake
  - More details: link
- WPA3 is recommended

Wi-Fi - WEP

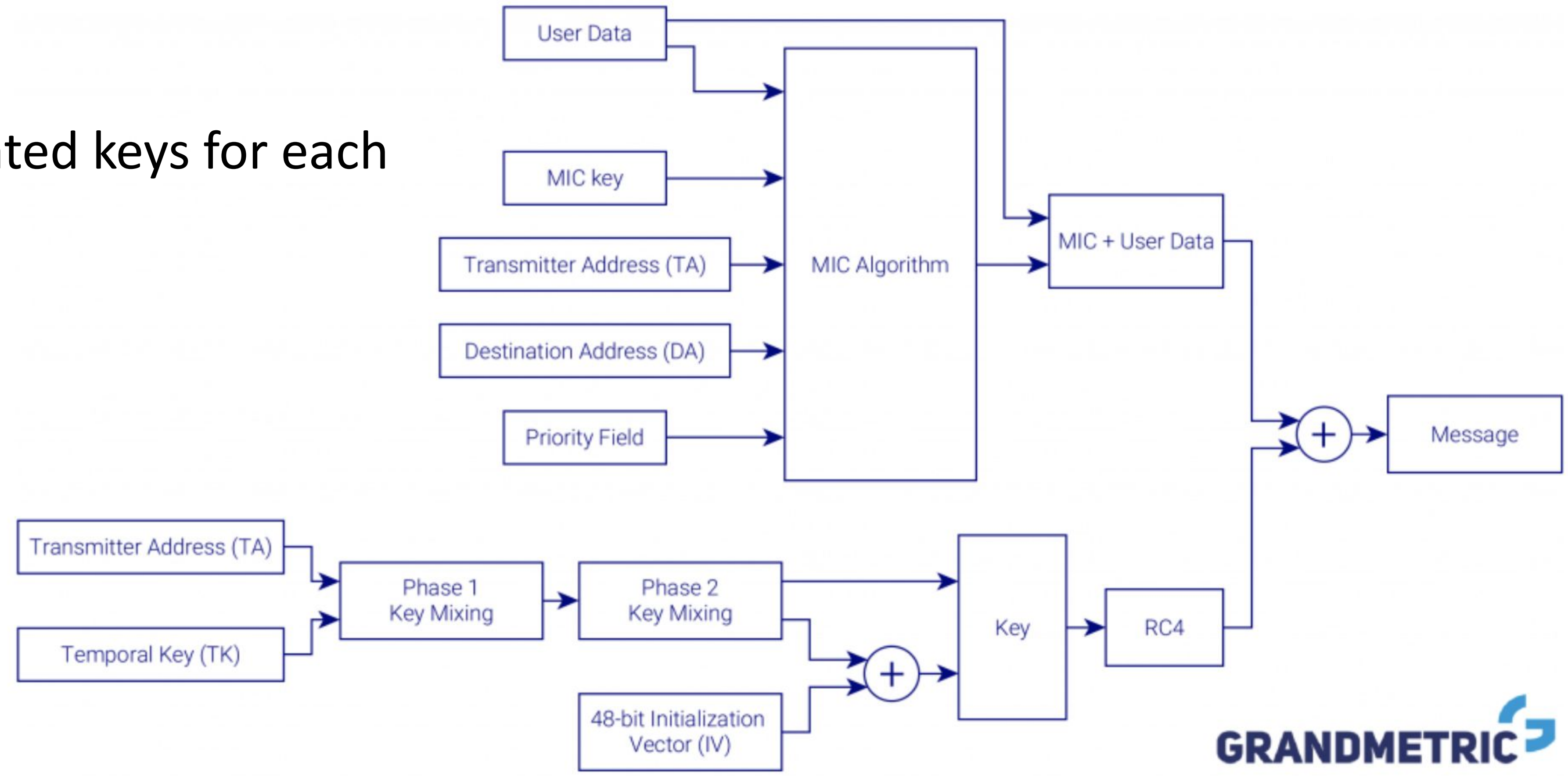
- RC4 cipher for encryption
- Open authentication - only encryption
- Shared key authentication - authentication + encryption
- Device authentication - four-step challenge-response handshake
- CRC32 for integrity
- Deprecated since 2004



WEP encryption scheme

Wi-Fi - WPA

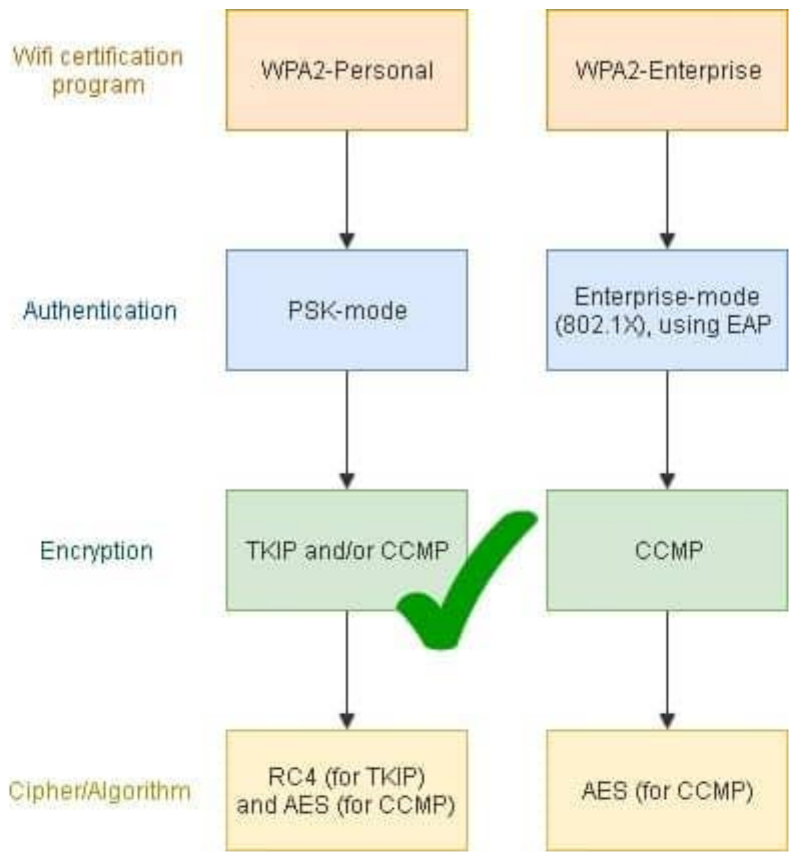
- RC4 cipher
- TKIP - 256 bit keys
- Dynamically generated keys for each packet
- MIC for integrity



Wi-Fi Security WPA encryption scheme

Wi-Fi - WPA2

- AES-CCMP for encryption
- TKIP - compatibility with WPA
- 4 phases to create secure communication
  - agree on security policy
  - generate master key
  - generate temporal keys
  - use CCMP to provide data integrity and confidentiality
- WPA2-Personal
  - PSK
- WPA2-Enterprise
  - 802.1X, EAP



Source: https://www.comparitech.com/blog/information-security/wpa2-aes-tkip/

WiFi - WPA3

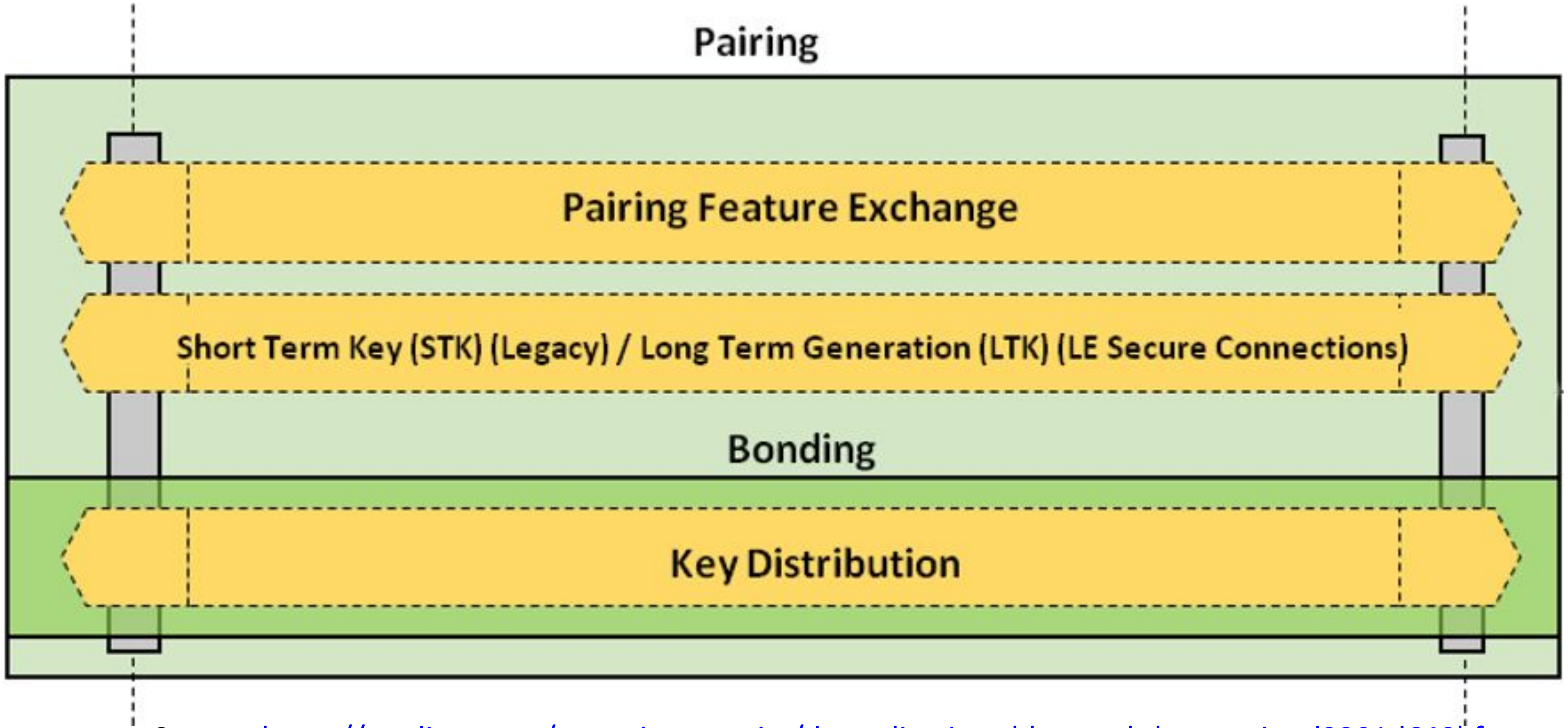
- AES with GCMP for encryption
- SAE for authentication
  - improves the security of initial key exchange
  - better protection against offline dictionary-based attacks
  - variation of dragonfly handshake
  - replacement for PSK (WPA2)
  - considers devices as equals
  - either device can initiate a handshake
  - forward secrecy

WiFi - WPA3

- WPA3 Personal
  - 128-bit encryption: AES-CCMP 128
- WPA3 Enterprise Mode
  - 128-bit mode
    - Authentication: EAP
    - Authenticated encryption: AES-CCMP 128
    - Key derivation and confirmation: HMAC-SHA256
    - Management frame protection: BIP-CMAC-128
  - 192-bit mode
    - Authentication: EAP-TLS with ECDH and ECDSA
    - Authenticated encryption: GCMP-256
    - Key derivation and confirmation: HMAC-SHA384
    - Management frame protection: BIP-GMAC-256

Bluetooth Low Energy (BLE)

- Each connection has a Security Mode and a Security Level
- Pairing
- STK
- LTK
- Bonding
- AES-CCM
- Digital signatures



Source: https://medium.com/rtone-iot-security/deep-dive-into-bluetooth-le-security-d2301d640bfc

BLE - Security Modes

- Security Mode 1
  - Level 1: No Security
  - Level 2: Unauthenticated pairing with encryption
  - Level 3: Authenticated pairing with AES-CCM encryption
  - Level 4: Authenticated LE Secure Connections pairing with encryption. ECDH and AES-CCM
- Security Mode 2
  - Level 1: Unauthenticated pairing with data signing
  - Level 2: Authenticated pairing with data signing
- Mixed Security Mode
  - support both Security Mode 1 and 2

BLE - Pairing modes

- Pairing = authenticating the identity of 2 devices
- After that, link is encrypted and keys are distributed
- Phase 1:
  - Communicate capabilities in Pairing Request message
  - No Input No Output, Display Only, Display Yes/No, Keyboard Only and Keyboard Display
- Phase 2:
  - LE Legacy: generate Short Term Key (STK)
  - LE Secure Connections: generate Long Term Key (LTK)
- Phase 3:
  - Generate LTK if it was not generated in phase 2
  - Generate other keys (CSRK, IRK)
  - Distribute keys

BLE - Pairing Methods

- Devices negotiate the Short Term Key
- Just Works
  - generated on both sides, based on the packets exchanged in plain text
  - no protection against MITM
- Passkey Display
  - one device displays a randomly generated 6-digit passkey
  - the other asks to enter the passkey
  - no display -> enter the same passkey on both
  - protection against MITM

BLE - Pairing Methods

- Out of Band (OOB)
  - data for generating the key is transmitted through other communication channel
  - for example NFC
  - protection against MITM
- Numeric Comparison
  - BLE 4.2
  - LE Secure Connections Pairing
  - ECDH for key generation
  - New pairing method
  - LTK generated in phase 2 and used to encrypt messages

BLE - Bluetooth 4.2

- New security model = LE Secure Connections
- ECDH for key generation
  - public/private key pairs
- Protects against passive eavesdropping
  - Numeric Comparison, Just Works, Passkey Entry, Out Of Band
- Protects against MITM attacks
  - Numeric Comparison, Passkey Entry, Out Of Band

Bibliography

- D. Dragomir, L. Gheorghe, S. Costea and A. Radovici, "A Survey on Secure Communication Protocols for IoT Systems," 2016 International Workshop on Secure Internet of Things (SIoT), 2016, pp. 47-62. (link)
- M Shila, Devu & Cao, Xianghui & Cheng, Yu & Yang, Zequ & Zhou, Yang & Chen, Jiming. (2014). Ghost-in-the-Wireless: Energy Depletion Attack on ZigBee.
- https://datatracker.ietf.org/doc/html/rfc3610
- https://www.krackattacks.com/
- https://www.wi-fi.org/discover-wi-fi/security
- https://www.grandmetric.com/2018/07/06/ended-wpa3-wi-fi-security-evolution/
- https://spectrum.ieee.org/everything-you-need-to-know-about-wpa3
- https://medium.com/rtone-iot-security/deep-dive-into-bluetooth-le-security-d2301d640bfc