IoT
Sensor Node Crunch

Embedded Systems Laboratory

Internet of Things

Lecture 7 - Standardized Security Solutions for IoT

Main Challenges

- Very large attack surface and widespread deployment
- Limited device resources
- Security by design was 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
  - 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

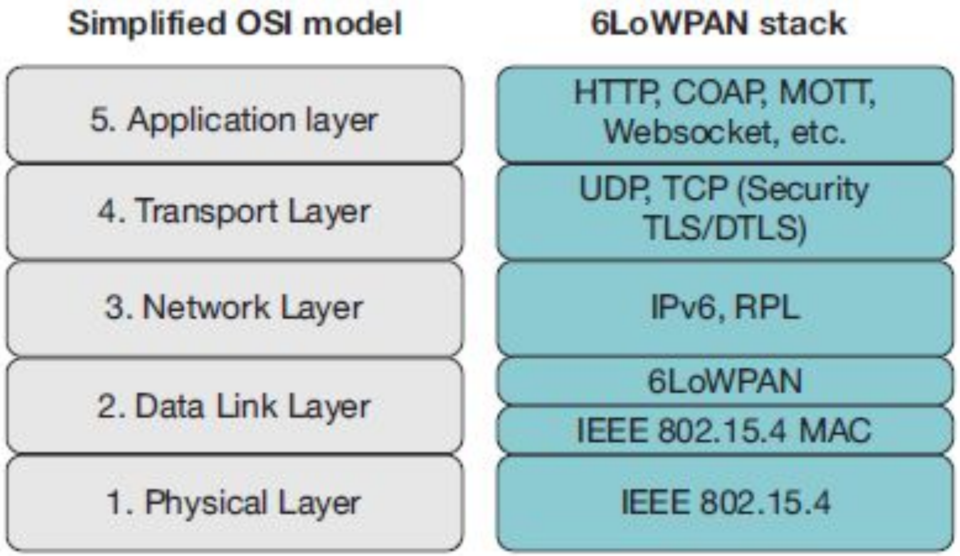


Table 1: IoT stack with standardized security solutions.

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

IEEE 802.15.4 Security

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

- Message Authentication Code - MAC (aka MIC)
- Computed based on the message and pre-shared secret key
- MAC sent with the message
- Receiver recomputes and verifies MAC
- AES-CBC-MAC and AES-CCM with 3 MAC lengths
    - 32, 64, 128 bits

IEEE 802.15.4 - Data confidentiality

- Encryption
- Semantic security using a nonce
  - Counter or random value
  - Differentiate between similar or identical messages
  - Sent in the packet, in plaintext
- AES-CTR and AES-CCM
  - 13 bytes nonce
  - Source address (8 bytes) + frame counter (4 bytes) + security control field (1 byte)

IEEE 802.15.4 - Replay Protection

- Anti-replay protection
- Frame counter
  - Incremented at each message
  - Receiver rejects msgs with smaller sequence numbers
  - Efficiency based on counter roll over
  - 32 bits counter
  - Part of nounces

IEEE 802.15.4 - Access Control

- Access control list (ACL)
  - List of valid devices
  - Verify source address of packets
  - Only packets from valid sources are forwarded
  - Easily bypassed by spoofing attacks
    - Node pretends to be another valid node

RPL

RPL

- Several security mechanisms against routing attacks
- Secure RPL routing packets
- Security modes: unsecured, preinstalled, authenticated
- A bit specifies if the packet is secured or not
- Security section in RPL header -> security type
- Unsecured messages when lower layer provides security

RPL

- "unsecured" mode
  - clear text, no security
- "preinstalled" mode
  - keys are preinstalled on nodes
  - cryptographic algorithms
- "authenticated" mode
  - nodes receive keys from key authority after authentication
  - same security mechanisms as "preinstalled"

RPL

- Security Services
  - data authenticity
    - mandatory
    - MAC or digital signature
  - data confidentiality
    - optional
    - encryption
  - replay protection
    - optional
    - nonce

RPL

- AES-128 CCM
  - encryption & MAC
  - MAC on 32 & 64 bits
- RSA with SHA-256
  - signature on 2048 & 3072 bits
- AES-128 CCM nonce
  - incremented at each packet

	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

RPL

- Key Identifier Mode (KIM)
  - key type - symmetric (0,1,2) & asymmetric (3)
- Security Level (LVL)
  - cryptographic algorithms
- Consistency Check (CC)
  - anti-replay protection
  - nodes verify & synchronize counters

	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

CoAP + DTLS

CoAP + DTLS

- DTLS - transport layer security
  - end-to-end security
  - data confidentiality and integrity, authentication
  - non-repudiation, anti-replay protection
  - over UDP
- CoAP with DTLS support

CoAP + DTLS

- Provisioning phase
  - Device identifiers are collected
  - Identifiers list => ACL
  - Devices receive keys and ACL

CoAP + DTLS

- 4 security modes: NoSec, PreSharedKey, RawPublicKey, Certificates
- NoSec - no DTLS, just UDP
- PreSharedKey
  - pre-programmed with symmetric shared keys
  - each device has a list of shared keys
  - keys used to communicate with other nodes/groups of nodes
  - DTLS in PSK mode
  - TLS_PSK_WITH_AES_128_CCM_8 cipher suite

CoAP + DTLS

- RawPublicKey
  - pre-programmed with asymmetric key pair
  - node identity - public key
  - keys compatible with ECDSA
  - SHA-256 for hashing
  - TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 cipher suite

CoAP + DTLS

- Certificates
  - asymmetric keys
  - X.509 certificate signed by trust root
  - devices have a list of trust anchors to validate certificates
  - device authentication - signature (ECDSA and SHA-256)
  - key agreement using ECDHE
  - TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 cipher suite

CoAP + DTLS

- ECC used in 2 security modes
  - strong security
  - small keys
  - less processing power
  - ECC with 160 bit keys ~ RSA with 1024 bit keys (ECC is 15x faster)
  - suitable for IoT

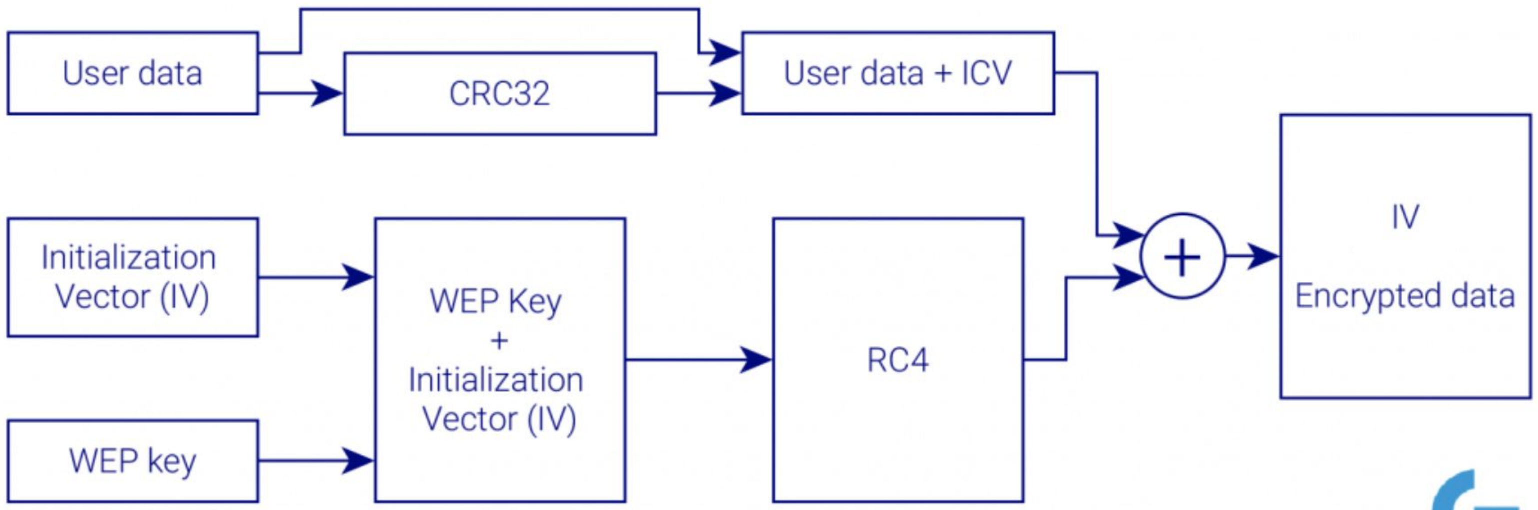
Wi-Fi

Wi-Fi

- More and more used in IoT
- Security protocols: WEP, WPA, WPA2, WPA3
- Krack attack for WPA2
  - replay attack
  - vulnerability in the 4-way handshake
  - continuously retransmit the 3rd message
  - key is exposed
- WPA3 is recommended

Wi-Fi - WEP

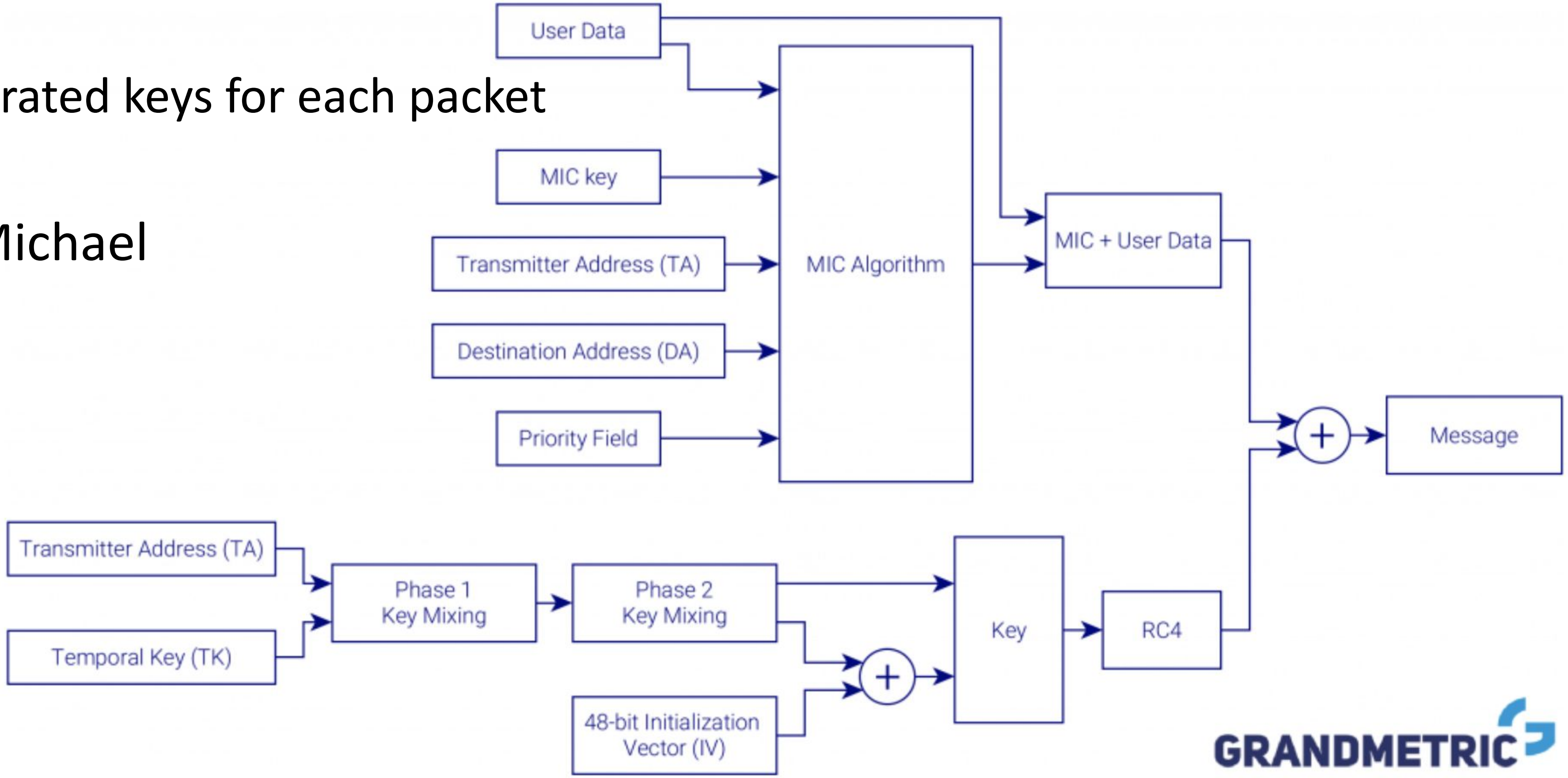
- RC4 stream cipher for encryption
- Open authentication - no credentials, only encryption
- Shared key authentication - authentication(user/pass) + encryption (64/128b keys)
- Device authentication - four-step challenge-response handshake
- CRC32 for integrity
  - Easy to compromise
- Deprecated since 2004



WEP encryption scheme

Wi-Fi - WPA

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



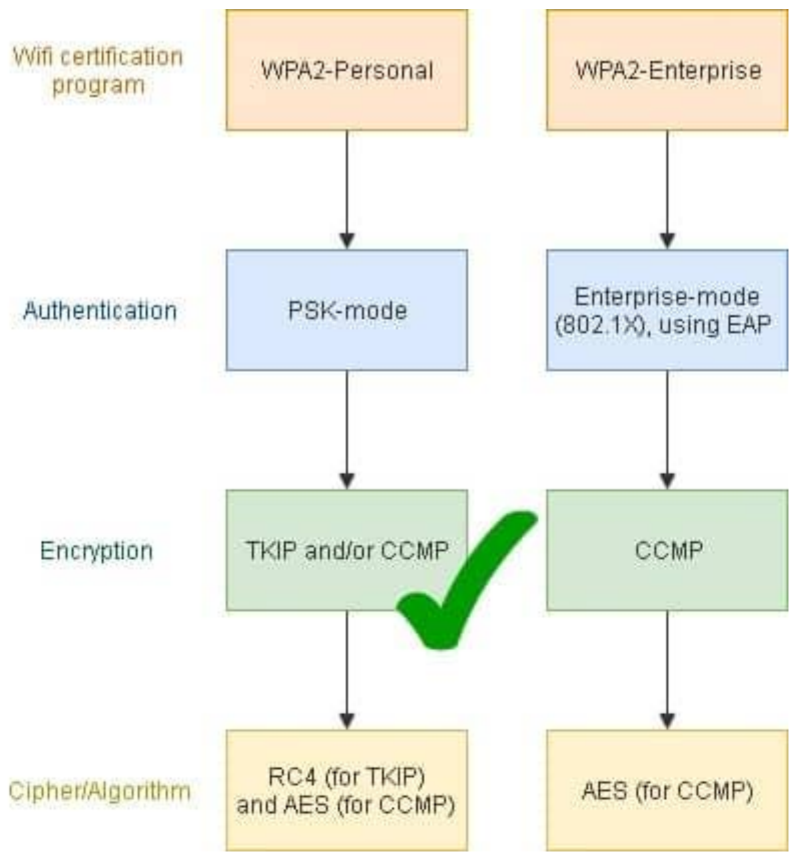
Wi-Fi Security WPA encryption scheme

Wi-Fi - WPA2

- AES-CCMP for encryption
  - 128 bit keys
- TKIP - only for compatibility with WPA
- 4 phases to create secure communication
  1. C&AP agree on security policy
  2. generate master key
  3. generate temporal keys
  4. use CCMP & temporal keys for data integrity & confidentiality

Wi-Fi - WPA2

- WPA2-Personal
  - PSK for authentication
  - shared key introduced by user on the client
- WPA2-Enterprise
  - 802.1X - username/password or certificate
  - Server AAA (RADIUS) - centralized authentication
  - EAP to send authentication messages
- Personal supports TKIP, Enterprise does not
- Personal for homes, Enterprise for companies



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

WiFi - WPA3

- 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 - KRACK attack)
  - considers devices as equals
  - either device can initiate the handshake
  - each device sends authentication info independently
  - forward secrecy - password is changed for every connection

WiFi - WPA3

- WPA3 Personal
  - 128-bit encryption
  - Authenticated encryption - AES-CCMP 128
- WPA3 Enterprise
  - 128-bit mode
    - Device authentication: EAP
    - Authenticated encryption: AES-CCMP 128
    - Key derivation: HMAC-SHA256
    - Management frame protection: BIP-CMAC-128

WiFi - WPA3

- WPA3 Enterprise Mode
  - 192-bit mode
    - Device authentication: EAP-TLS with ECDH and ECDSA
    - Authenticated encryption: GCMP-256
    - Key derivation: HMAC-SHA384
    - Management frame protection: BIP-GMAC-256
    - Stronger security
  - Cannot be used on resource constrained devices

BLE

Bluetooth Low Energy (BLE)

- Each connection has a Security Mode and a Security Level
- Pairing
  - initiated by a central device
  - mutual device authentication
  - encrypt traffic using short-term key (STK)
  - distribute long-term keys (LTK)
  - LTK saved for rapid reconnection (bonding)

Bluetooth Low Energy (BLE)

- Encryption - AES-CCM
  - LTK + AES-CCM => secret shared key (128b)
- Authentication - digital signatures
  - Connection Signature Resolving Key (CSRK)
- Generic Access Protocol (GAP)
  - 2 security modes with multiple security levels
  - each connection starts at mode 1 level 1
  - update to another level depending on the authentication method
  - the authentication method is decided during pairing

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 (Bluetooth 4.2)
- 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

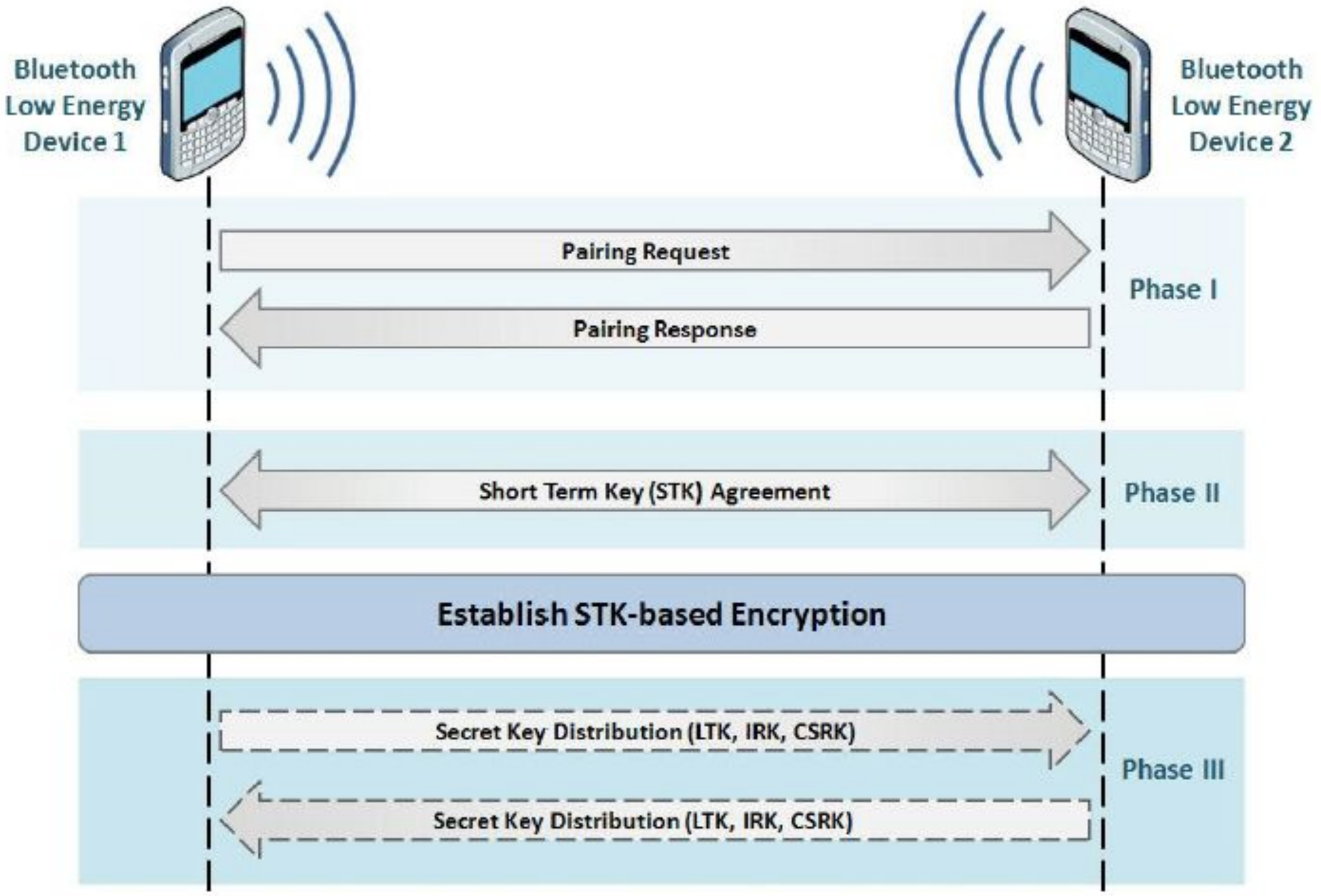
BLE - Pairing modes

- Pairing = authenticating the identity of 2 devices
- After that, link is encrypted and keys are distributed
- Keys are saved => Bonded devices, fast reconnect
- Pairing - 3 phases
- Phase 1:
  - communicate capabilities in Pairing Request message
  - No Input No Output, Display Only, Display Yes/No, Keyboard Only and Keyboard Display
  - determine the pairing method (phase 2)

BLE - Pairing modes

- Phase 2:
  - LE Legacy: generate Short Term Key (STK)
    - using a Temporary Key + random numbers
  - LE Secure Connections: generate Long Term Key (LTK)
- Phase 3:
  - Generate LTK if it was not generated in phase 2 (Legacy)
  - Generate other keys (CSRK, IRK)
  - Distribute keys

BLE - Legacy Pairing



Source: https://www.researchgate.net/publication/311611851_Exploiting_Bluetooth_Low_Energy_Pairing_Vulnerability_in_Telemedicine

BLE - Pairing Methods

- Devices negotiate the Short Term Key
- 4 methods - depending on device capabilities
- Just Works
  - generated on both sides, based on the packets exchanged in plain text
  - no protection against MITM

BLE - Pairing Methods

- 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
- Out of Band (OOB)
  - data for generating the key is transmitted through other communication channel
  - e.g. NFC
  - protection against MITM

BLE - Pairing Methods

- Numeric Comparison
  - BLE 4.2
  - LE Secure Connections Pairing
  - ECDH for key generation
  - New pairing method for key exchange
  - 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