OpenWeave
Security

OpenWeave Security Goals

Secure device communication

- Independent of the underlying transport
  - Thread, Wi-Fi, Ethernet, Cellular, BTLE
- For different types of devices
  - Constrained power (coin cell), memory (as little as 64kB RAM), CPU. Unconstrained
- For different types of operations
  - Pairing, device-to-device, device-to-service, service-to-device
- Across application domains
  - HVAC, safety, security, sensors

Overview

Most messages encrypted with shared key crypto

- leverage ubiquitous AES HW acceleration

Sparing use of public key crypto

- emphasis on memory-efficient elliptic curve methods

Strong identity tied to a certificate

Different session establishment protocols

- human friendly -- use passcode
- machine friendly -- certificates

Application keys -- long lived, secure key management for groups of devices

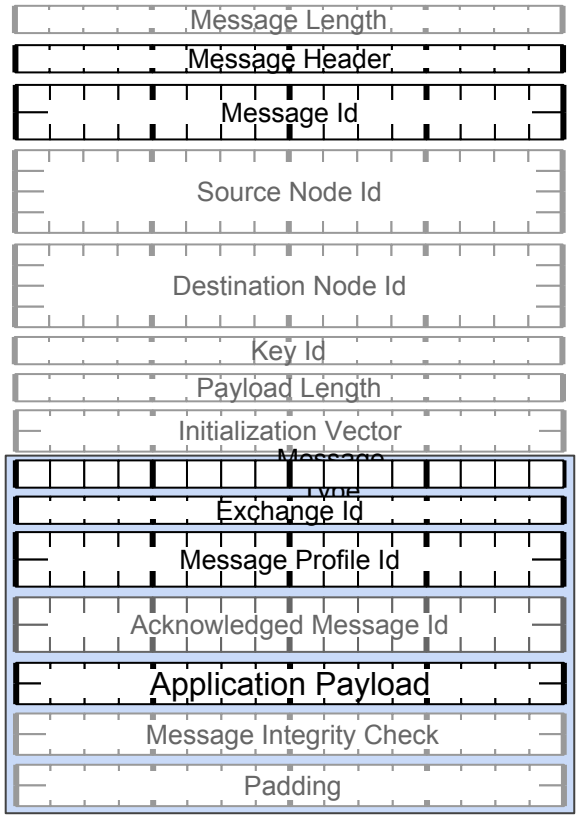
OpenWeave Message Encryption / Authentication

Encryption / Authentication is built-in to Weave Message Architecture

- AES-128 encryption
- CTR-mode stream cipher
- HMAC-SHA1 integrity
- Separate keys for encryption / integrity
- Key sources:
  - Short-term peer-to-peer session keys
  - Long-term group keys
- Extensible

OpenWeave Message Encryption / Authentication

- Fields Subject to Encryption
  - message type and profile
  - exchange information
  - message acknowledgment info
  - message integrity code
  - application payload
- Fields Subject to Integrity
  - application payload
  - message type and profile
  - exchange information
  - message acknowledgment info
  - source / destination node ids
  - message version



Grey denotes optional or conditional fields.
Blue denotes fields subject to encryption.

OpenWeave Message Encryption / Authentication

Categories of keys used to secure messages

- Session keys
  - Negotiated on as-needed basis
  - Generated via session establishment protocols (CASE, PASE)
  - Two-party only
  - Generally short lived
- Group / fabric keys
  - Established at joining time
  - Shared by all / some nodes in fabric
  - Long lived
  - Subject to rotation
  - Session key support well developed
  - Group key support rudimentary

Password Authenticated Session Establishment (PASE)

- Weave protocol for mutual authentication / session establishment based on low-entropy passwords
- Based on J-PAKE cryptographic protocol (finite-field and EC)
- Crypto features
  - Resistant to man-in-the-middle attacks
  - Does not reveal any part of password
  - Perfect forward security
- Uses
  - App-to-device (Weave pairing, thread commissioning)
  - Device-to-device (Nest Thermostat to HeatLink pairing)
  - Crypto-proof completed by Google security team

Certificate Authenticated Session Establishment (CASE)

- Weave protocol for mutual authentication / session establishment based on peer certificates
- Based on ECDH and ECDSA (Weave certificates)
- Support for NIST-192, 224 and 256 bit curves
- Simplified (but flexible) certificate path validation
- No support for CRLs
- Uses
  - App-to-device (pairing)
  - Device-to-service (all interactions)
  - Device-to-device (in-field joining)

Certificates

Simplified / Compact X.509 v3 Certificates

- Constrained features
  - 1-level distinguished name
  - EUI-64s used as naming attributes
  - Limited support for extensions
- Compressed encoding using Weave TLV
  - 30% smaller than X.509 DER form
  - lossless conversion to/from X.509
- CA signature based on X.509 DER form, not TLV form
- Can be used in standard protocols (TLS)
- Design optimizes code and data space on devices

Certificates for Devices and Authentication

Weave Certificates for Devices

- Certificate subject name is Weave device id (802.15.4 MAC)

  `/WeaveDeviceId=18B4300000000001`

- Signed by Nest Device CA certificate
- Certificate and private key provisioned onto device during manufacturing
- Used by devices to prove their identity to service, mobile apps
- Also provides proof of device authenticity
- Peers trust device certificate based on trusting Nest root certificate

Certificates for Service Endpoints

Weave Certificates for Services

- Certificate subject name is service endpoint id (EUI-64)

  `/WeaveServiceEndpointId=18B4300200000003`

- Signed by Nest Service Endpoint CA certificate
- Installed on server instances in Nest service
- Used by servers to prove their identity to devices
- Also provides proof of device authenticity
- Peers (devices) trust service endpoint certificates based on trusting the service root certificate contained in the service config

Certificates for Firmware Signing

Weave Certificates for Software Publishers

- Certificate subject name is service endpoint id (EUI-64)

  `/WeaveSoftwarePublisherId=18B4300302000001`

- Signed by Nest Firmware Signing CA certificate
- Installed on official build machines
- Firmware images include signing certificate + CA certificate
- Devices trust firmware images based on trusting the Nest root certificate

Nest Trust Domain

- Nest X.509-based PK Hierarchy
  - Fairly typical organization
  - Single root certificate
- 3 CA certificates: device, service endpoint and firmware signing
  - EC keys (NIST P-224)
  - Administered by Nest
  - Multi-party key ceremonies

Token Authenticated Key Exchange (TAKE)

- Authentication protocol for BLE user tokens (fob, mobile)
- Based on ECDH / ECDSA plus symmetric keys
- Support auth-only and auth with session establishment
- Anonymous authentication of token
- Support for time-limited traceability privilege
- Plans to align keying system with Eddystone
- Uses
  - Device-to-device (disarm with fob)
  - Mobile-to-device (disarm with phone)

Application Keys

Symmetric Group Key Framework

- Generation/dissemination/management of shared group keys
- Flexible membership rules based on application security requirements
- Groups can include (or exclude): devices, mobiles and service
- Strong enforcement of group membership (with siloed administration)
- Common mechanism for key dissemination (WDM)
- Built-in key rotation scheme
- Uses
  - Device-to-device messaging (home security communication)
  - Mobile-to-device data encryption (passcodes)
  - Mobile-to-device commands (physical access control)

Summary

Full featured, robust security, fits the smallest devices

Supports all types of devices operations independent of transport

Collection of different security mechanisms can support many different application domains.