6TiSCH
Internet-Draft
Intended status: Informational
Expires: January 5, 2015

R. Struik
Struik Security Consultancy
July 4, 2014

6TiSCH Security Architectural Elements
draft-struik-6tisch-security-architecture-elements-00

Abstract

This document describes security architectural elements that are relevant for the design of the 6TiSCH security architecture. (Note: this document is a work-in-progress and will provide more fine-tuned information with updated versions.)

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of This Memo

Copyright Notice

Table of Contents

1. Preliminaries

1.1. Device Roles

When discussing security operations, it is useful to distinguish various device roles. Here, one should note that a device may assume more than one device role at the same time and that a particular role may be assumed by more than one device. Moreover, the mapping of device roles to devices may change over time (along a device's or network's lifecycle).

We distinguish the following roles:

1. Client. This device may move in and out of networks (that may be alien to it) and may have little network management functionality on board. Key words: nomadic, promiscuous, constrained.

2. Access point. This device may be more tied into a relatively stable infrastructure and may have more support for network management functionality or have reliable access hereto (e.g., via a back-end system). Key words: anchor, semi-stable connectivity, access portal.

3. Server. This device provides stable infrastructure and network management support, either intra-domain or inter domain (thereby, offering homogeneous or even heterogeneous functionality). Key words: core function, high availability, human-operator support.

4. CA. This device vouches for trust credentials, usually in offline way. Key words: trust anchor.

1.2. Initiator and Responder Model

All peer-to-peer protocols are role-symmetrical (i.e., the role of initiator/responder roles are interchangeable). Protocols involving a third party assume communications with this third party to take place via the access point (since being the device more tied into infrastructure).

1.3. Cautionary Note - on Limitations of Cryptography

Cryptographic techniques may provide logical assurances as to a device’s identity, where and when communications originated, whom it was intended for, whom this can be read by, etc.

Cryptographic techniques do, however, only provide mechanical assurances and can generally not substitute human authorization decision elements (unless the latter are not important, such as with random, ad-hoc networks).

1.4. Desired Protocol Properties

Security-Related:

1. Parties executing a security protocol should be explicitly aware of its security properties

2. Compromise of keys or devices should have limited effect on security of other devices or services

3. Attacks should not have a serious impact beyond the time interval/space during/in which these take place

4. Security protocols should minimize the impact of network outages, denial of service attacks

Communication Flows:

1. Security protocols should allow to be run locally, without third party involvement, if at all possible

2. The number of message exchanges for a joining client device should be reduced

3. Message exchanges should be structured so as to allow parallel execution of protocol steps, if possible

Computational Cost:

1. Security protocols should not impose an undue computational burden, esp. on joining client devices (An exception here may arise, when recovering from an event seriously impacting availability of the network.)

Device Capabilities:

1. Dependency on an accurate time-keeping mechanism should be reduced

2. Computational/time latency trade-offs should be tweaked to benefit those of joining client, if possible

3. Dependency on "homogeneous trust models" should be reduced, without jeopardizing security properties

4. Dependency on on-board trusted platforms and trusted I/O interfaces should be reduced

1.5. Device Enrolment Phases

1. Device Authentication. Client A and Access Point B authenticate each other and establish a shared key (so as to ensure on-going authenticated communications). This may involve server KDC as third party.

2. Authorization. Access Point B decides on whether/how to authorize device A (if denied, this may result in loss of bandwidth). Authorization decision may be delegated to server KDC or other 3rd-party device.

3. Configuration/Parameterization. Access Point B distributes configuration information to Client A, such as

   * IP address assignment info;

   * Bandwidth/usage constraints;

   * Scheduling info (including on re-authentication policy details)

This may originate from other network devices, for which it acts as proxy. This step may also include distribution of information from Client A to Access Point B and, more generally, synchronization of information between these two entities.

The device enrollment process is depicted in Figure Figure 1, where it is assumed that devices have access to certificates and where entities have access to the root CA key of its communicating parties (initial set-up requirement). Under these assumptions, the authentication step of the device enrollment process does not require online involvement of a third party.

```
{joining node}      {neighbor}                 {server, etc.}
+---------+         +---------+                 +---------+
| Client  |         | Access  |              +--|    CA   |e.g., certificate
|    A    |         | Point B |              |  +---------+       issuance
+---------+         +---------+              |  +---------+
    |                    |                   +--|Authoriz.|e.g., membership
    |<----Beaconing------|                   |  +---------+         test
    |                    |                   |  +---------+
    |<--Authentication-->|                   +--| Routing |e.g., IP address
    |                    |<--Authorization-->|  +---------+       assignment
    |<-------------------|                   |  +---------+
    |                    |                   +--| Gateway |e.g., backbone,
    |------------------->|                   |  +---------+      cloud
    |                    |<--Configuration-->|  +---------+
    |<-------------------|                   +--|Bandwidth|e.g., PCE schedul
e
    .                    .                   .  +---------+
    .                    .                   .
```

Figure 1: Networking Joining, with Only Authorization by Third Party

Aggressive scheme: Initiate authorization/configuration processes as soon as (presumed) device identity becomes available (invisible to Client A). Access Point B can deny bandwidth if authorization negative.

Note: Communication of configuration info depends on secure channel with Client A.

1.6. Security Definitions

1. Key Establishment: Protocol whereby a shared secret becomes available to two or more parties for subsequent cryptographic use

2. Key Transport: Key establishment technique where one party creates/obtains the secret and securely transfers it to other(s)

3. Key Agreement: Key establishment technique where the shared secret is derived based on information contributed by each of the parties involved, ideally so that no party can predetermine this secret value

4. Implicit Key Authentication: Assurance as to which specifically identified parties possibly may gain access to a specific key

5. Key Confirmation: Assurance that second (possibly unknown) party has possession of a particular key

6. Explicit Key Authentication: Combination of implicit key authentication and key confirmation

7. Unilateral Key Control: Key establishment protocol whereby one party can influence the shared secret

8. Forward Secrecy: Assurance that compromise of long-term keys does not compromise past session keys

9. Entity Authentication: Assurance of active involvement of second explicitly identified party in protocol

10. Mutual vs. Unilateral: Adjective indicating symmetry, resp. asymmetry, of assurances amongst parties

11. Identity Protection: Assurance as to which specifically identified parties may gain access to identity info

12. Certificate ? Credential that vouches for authenticity of binding between a public key and other information, including the identity of the owner of the public key in question

13. Key Possession? Assurance that a specific (possibly unknown) party has possession of a particular key

Esoteric properties: Unknown Key Share Resilience, Session Key Retrieval, Key Compromise Impersonation

1.7. Deployment Scenarios

Deployment scenarios discussed with industrial control user community:

1. Scenario #1: mix-and-match of nodes from different vendors

2. Scenario #2: addition of nodes to operational network

3. Scenario #3: security audit

4. Scenario #4: device repair and replacement (roaming in/out different user sites)

5. Scenario #5: network separation (devices joining wrong network)

6. Scenario #6: thwarting malicious attacks by (former) insiders

7. Scenario #7: thwarting attacks by outsiders via insiders (held at 'gunpoint')

8. Scenario #8: addition of subsystem ('skid') assembled elsewhere to operational network

2. Security Considerations

This document is all about security.

3. Other Related Protocols

4. IANA Considerations

5. Acknowledgements

Discussions amongst participants in the 6TiSCH security conference calls to-date helped to shape this document.

6. References

6.1. Normative references

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC6550] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, March 2012.

[RFC6775] Shelby, Z., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, November 2012.

[RFC7250] Wouters, P., Tschofenig, H., Gilmore, J., Weiler, S., and T. Kivinen, "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", RFC 7250, June 2014.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, June 2014.

[I-D.ietf-6tisch-coap] Sudhaakar, R. and P. Zand, "6TiSCH Resource Management and Interaction using CoAP", draft-ietf-6tisch-coap-00 (work in progress), May 2014.

[I-D.ietf-6tisch-architecture] Thubert, P., Watteyne, T., and R. Assimiti, "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4e", draft-ietf-6tisch-architecture-02 (work in progress), June 2014.

[I-D.wang-6tisch-6top-sublayer] Wang, Q., Vilajosana, X., and T. Watteyne, "6TiSCH Operation Sublayer (6top)", draft-wang-6tisch-6top-sublayer-00 (work in progress), February 2014.

[I-D.ietf-6tisch-6top-interface] Wang, Q., Vilajosana, X., and T. Watteyne, "6TiSCH Operation Sublayer (6top) Interface", draft-ietf-6tisch-6top-interface-00 (work in progress), March 2014.

6.2. Informative references

[I-D.garcia-core-security] Garcia-Morchon, O., Kumar, S., Keoh, S., Hummen, R., and R. Struik, "Security Considerations in the IP-based Internet of Things", draft-garcia-core-security-06 (work in progress), September 2013.

[I-D.ietf-dice-profile] Hartke, K. and H. Tschofenig, "A DTLS 1.2 Profile for the Internet of Things", draft-ietf-dice-profile-01 (work in progress), May 2014.

[I-D.kumar-dice-dtls-relay] Kumar, S., Keoh, S., and O. Garcia-Morchon, "DTLS Relay for Constrained Environments", draft-kumar-dice-dtls-relay-01 (work in progress), April 2014.

[I-D.thubert-6lowpan-backbone-router]
Thubert, P., "6LoWPAN Backbone Router", draft-thubert-6lowpan-backbone-router-03 (work in progress), February 2013.

[IEEE802.15.4-2011]
Institute for Electrical and Electronics Engineers, "IEEE 802.15.4-2011, IEEE Standard for Local and Metropolitan Area Networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)", September 2011.

[IEEE802.15.4e-2012]
Institute for Electrical and Electronics Engineers, "IEEE 802.15.4e-2012, IEEE Standard for Local and Metropolitan Area Networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), Amendment 1: MAC Sublayer", April 2012.

[Wireless-HART]
International Electrotechnical Commission, "IEC 62591, Ed. 2.0: Industrial Communication Networks - Wireless Communication Network and Communication Profiles - WirelessHART (Draft)", November 2013.

[ISA100.11a]
International Electrotechnical Commission, "IEC 62734, Ed. 1: Industrial Communication Networks - Wireless Communication Network and Communication Profiles - ISA 100.11a (Draft)", May 2013.

[ZigBee-IP]
ZigBee Alliance, "ZigBee IP Specification (ZigBee Public Document 13-002r00)", February 2013.

Author's Address

Rene Struik
Struik Security Consultancy

Email: rstruik.ext@gmail.com