Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 04, 2014

M. Richardson
SSW

March 03, 2014

security architecture for 6top: requirements and structure
draft-richardson-6tisch-security-architecture-01

Abstract

This document details minimal layer-2 requirements for 6top use in industrial settings, and a few options for accomplishing this. The layer-2 mechanism is then extended to provide for per-node authentication and authorization of the node/PCE communications. This internet-draft is intended for later inclusion into the 6tisch architecture document.

This might be the worst written internet draft yet. You have been warned

Table of Contents

1. Introduction: security bootstrap requirements

2. Requirements Language

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

3. layer-2 security requirements

As outlined in [I-D.ietf-roll-security-threats] there are a number of threats in LLNs, and in RPL which are solved if there is layer-2 security. The requirement is therefore to provide keying for the layer-2 security features: encryption and integrity protection.

In addition to serving to protect the routing traffic against attacks, use of the layer-2 access control serves as adminission control to the network. It is therefore part of the layer-2 join process to authenticate the new node, as well as authorize it to join the network. The admission control SHOULD be controlled by autonomic certificates, see section X.

4. 6top/PCE security requirements

In addition to authorization a node to join the network, the node agree to provide authorization to a PCE in order for the 6top protocol to run. This protocol, described in section X of 6tisch architecture (this) document and in [6top], permits the PCE to program a timeslot schedule into the node.

So, the second part of the 6tisch security requirements is to establish the identities of the the node and the PCE, and to establish an authorization that permits the new node to be programmed by the PCE.

5. leveraging layer-2 identities for layer-4 security

As explained in [I-D.behringer-autonomic-network-framework] the layer-2 identity of the node will be given by a certificate signed by the vendor of the node. The vendor's certificate authority is loaded into the (PANA) Authorization Server, and permits the AS to authenticate the node.

The vendor provides a certificate (chain) to the (PANA) Authorization Server (PAS) attesting to that the PAS is the rightful owner/ controller of the node. This permits the node to validate that the network it is joining is the correct network. This process permits the bootstrap of one of the layer-2 security mechanism(s) describe in sections below.

The same set of trust relationships can then permit the PAS to act as an Authorization Server (now, in the context of [I-D.gerdes-core-dcaf-authorize]). The PCE and it's Authorization Manager (AM, again from [I-D.gerdes-core-dcaf-authorize]) can now get a ticket to permit it to write the timeslot schedule. In option 2, below, it also permits updates to the security parameters.

6. option 1: The ZigBeeIP/PANA way

This is an adaptation of the process described in [ZigBeeIP], section and expounded upon in section 6.3: "Network Discovery", 6.4: "Network Selection", and 6.5, "Node Joining". The process is abridged below.

6.1. Network Discovery

The MAC beacon facility is used. A critical difference in 6tisch from ZigBee IP is that because nodes transmit and receive according to their own schedule, every node is in essence a coordinator. While nodes may sleep a lot, they will not in general be sleep Hosts, from a ZigBee IP point of view, and MLE is not necessary.

Each response to the Beacon is a potential network-joining-parent.

As an option, it may be desireable for this document to define a well known NetworkID.

6.2. PANA protocol

The PANA payloads MUST be relayed by the chosen network-joining-parent. It is assumed that the PANA Authentication Agent is co-located with the PCE, if there is a PCE.

As per section 8.3.4 of [ZigBeeIP], the PANA process runs over UDP using link-layer addressing. The process is first the PANA initialization (PCI, PAR:S, PAN:S), followed by EAP initialization (EAP-Request, EAP-Response), which negotiates the identity, and then EAP-TLS starts, consisting of (TLS(Start), TLS(ClientHello), TLS(ServerHello), TLS(ServerKeyExchange), TLS(ClientKeyExchange), and TLS(ChangeCipherSpec)).

When the TLS is done, the EAP derives new network security material, and sends it encrypted using the Encr-Encap AVP described in [RFC6786].

6.3. Authorization

QUESTION: can we find a way for the authorization protocol, such as described in draft-gerdes-core-dcaf-authorize-01, to run simultaenously with the authentication system if we assume that the dcaf AS is also the PANA Authentication Server/Agent

In the context of draft-selander-core-access-control, the new node that is joining is the resource server, and the origin client is the PCE.

7. option 2: The WirelessHart/ISA100 way

This is an adaptation of the process described in [HART], section 6.6.3.

In this process, the new node joins using a well-known layer-2 "JOIN" key. It brings up the layer-3, using 6loWPAN Neighbour Discovery to learn of the 6lowpan contexts, and then uses RPL to join a well-known DODAG as a leaf node.

Nodes which have capacity for new joining nodes will respond to the RPL DIS messages. Once connected, the new node uses regular unicasted IP datagrams to contact an Authorization Manager (in the context of [I-D.gerdes-core-dcaf-authorize]). The negotiation with the Authorization Manager (AM) uses the autonomic certificates as described above to establish the trust relationship.

Once the relationship is up, the AM needs to signal the PCE that it has a new authorized node, and the PCE can now (acting as a [I-D.gerdes-core-dcaf-authorize] Client), get a Ticket to update the node.

The PCE then writes both a new timeslot schedule, and also writes new security parameters that permit the node to fully join the network. Appropriate layer-2 keys are updated, as well as any appropriate layer-3 RPL credentials. MLE may be used to establish pair-wise keying, as appropriate to the timeslot schedule.

8. Security Considerations

9. Other Related Protocols

10. IANA Considerations

11. Acknowledgements

12. Normative references

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

[ZigBeeIP] ZigBee Public Document 15-002r00, "ZigBee IP Specification", 2013.

[RFC6786] Yegin, A. and R. Cragie, "Encrypting the Protocol for Carrying Authentication for Network Access (PANA) Attribute-Value Pairs", RFC 6786, November 2012.

[I-D.ietf-roll-security-threats] Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., and M. Richardson, "A Security Threat Analysis for Routing Protocol for Low-power and lossy networks (RPL)", draft-ietf-roll-security-threats-06 (work in progress), December 2013.

[I-D.behringer-autonomic-network-framework] Behringer, M., Pritikin, M., Bjarnason, S., and A. Clemm, "A Framework for Autonomic Networking", draft-behringer-autonomic-network-framework-01 (work in progress), October 2013.

[I-D.gerdes-core-dcaf-authorize] Gerdes, S., Bergmann, O., and C. Bormann, "Delegated CoAP Authentication and Authorization Framework (DCAF)", draft-

gerdes-core-dcaf-authorize-02 (work in progress), February 2014.

[HART] www.hartcomm.org, "Highway Addressable Remote Transducer, a group of specifications for industrial process and control devices administered by the HART Foundation", .

[ISA100.11a] ISA, "ISA100, Wireless Systems for Automation", May 2008, < http://www.isa.org/Community/SP100WirelessSystemsforAutomation>.

Author's Address

Michael C. Richardson
Sandelman Software Works
470 Dawson Avenue
Ottawa, ON K1Z 5V7
CA

Email: mcr+ietf@sandelman.ca
URI: http://www.sandelman.ca/