A YANG Model for Terminal Access Controller Access-Control System Plus (TACACS+) over TLS 1.3

draft-boucadair-opsawg-secure-tacacs-yang

IETF#120, Vancouver
July 2024

M. Boucadair (Orange)

Flashback

- *"RFC 8907 was published with informational status and it contained substantial caution in its security considerations that the protocol **was fundamentally insecure** and would not "meet modern-day requirements." This measured approach was taken to provide a stable description of a widely deployed protocol and **to serve as the basis for future improvements**"* (Roman Danyliw (SEC AD))

- When "A YANG Data Model for TACACS+" was proposed for publication back in 2021,
  - It was challenged because "*this functionality is new, and is not documenting the "as is" deployed state*" (Roman Danyliw (SEC AD))

  - "*My understanding is that RFC8907 defines the current TACACS+ protocol as it stands, and that this draft is intended to document the YANG configuration data model that goes alongside RFC8907, and that these two documents act **as a starting point for any future TACACS+ work in IETF***." (Rob Wilton (OPS AD))

Flashback

- “A YANG Data Model for TACACS+” was the published as RFC 9105, but with a warning

> This document defines a Terminal Access Controller Access-Control System Plus (TACACS+) client YANG module that augments the System Management data model, defined in RFC 7317, to allow devices to make use of TACACS+ servers for centralized Authentication, Authorization, and Accounting (AAA). ***Though being a standard module, this module does not endorse the security mechanisms of the TACACS+ protocol (RFC 8907), and TACACS+ MUST be used within a secure deployment.***

- and…

Flashback

```
choice encryptionsecurity {
  mandatory true;
  description
    "Security mechanism between TACACS+ client and server.
     This is modeled as a YANG 'choice' so that it can be
     augmented by a YANG module in a backwards-compatible
     manner.";
  case shared-secretobfuscation {
    leaf shared-secret {
      type string {
        length "1..max";
      }
      nacm:default-deny-all;
      description
        "The shared secret, which is known to both the
         TACACS+ client and server.  TACACS+ server
         administrators SHOULD configure a shared secret with
         a minimum length of 16 characters.
         It is highly recommended that this shared secret is
         at least 32 characters long and sufficiently complex
         with a mix of different character types,
         i.e., upper case, lower case, numeric, and
         punctuation.  Note that this security mechanism is
         best described as 'obfuscation' and not 'encryption'
         as it does not provide any meaningful integrity,
         privacy, or replay protection.";
      reference
        "RFC 8907: The TACACS+ Protocol";
    }
  }
}
```

A provision for future secure schemes

RFC 9105

So, Why Now?

- Because the WG has ***a good basis*** TACACS+TLS candidate
- It is the last mile to ***assess*** whether the ***manageability provisions*** in the TACACS+TLS are adequately covered
  - Simple reuse of TLS groupings may ***import complexity***, while this is not justified in this context
  - Add anchor text to the base specification

Scope

- The module is designed to cover the following key requirements specified in I-D.ietf-opsawg-tacacs-tls13
  - TLS 1.3 MUST be used for transport
  - Earlier TLS versions TLS MUST NOT be used
  - The cipher suites offered or accepted SHOULD be configurable
  - Implementations MAY support Raw Public Keys and PSK
  - Implementations MUST support the ability to configure the server’s domain name

Identifified Gaps

- I-D.ietf-opsawg-tacacs-tls13 need to be explicit about the ***intended behavior*** on some few items
  - Only a domain name is provisioned
  - When both a domain name and a list of addresses are provided (e.g., should that domain name passed to a resolution library)
  - Address selection procedure when a list of @ is available (e.g., should 8305 be followed)
  - keepalives

Issues & Next Steps

- ***Discussion#1***: RFC 9105bis *vs.* augment
  - The document is designed currently an augmentation to RFC 9105
  - Normative language for some new data nodes to take precedence over "address" and "port" data nodes defined in RFC 9105

- ***Discussion #2***: Pruning approach *vs.* reuse of the groupings in I-D.ietf-netconf-tls-client-server
  - Pruning is currently used to allow factorizing the same configuration for multiple server instances

- Consider WG Adoption