TACACS+ RFC Proposal

Presenters: Thorsten Dahm (Google), Andrej Ota (Google), Doug Gash (Cisco)

Agenda

v3

- TACACS+ Background
- Motivations for Standardization
- Proposed Changes
- Open Questions

TACACS+ Background

- Current Informal standard defined by TACACS+ Draft 1998
  - Standards Process Never completed.
- Widespread adoption for Device Administration Role:
  - Mediate the access of devices for configuration update.
  - Network Access Role delegated to RADIUS

Motivation for Standardization

- Impact of Lack of standardization:
  - TACACS+ seen as Cisco Proprietary Protocol
  - Completing process would help broaden adoption of TACACS+ for Device Administration.
- Cleanup of Standard
  - Deprecate Legacy Elements
  - Focus on Current Use Cases
  - Clarify/Disambiguate Text
- Take advantage of Process to update Transport Security

Proposed Changes: Transport Security

- Conflicting requirements:
  - Current Encryption (MD5) is not regarded as secure.
  - Full backwards compatibility Mandatory because of wide deployment
- Proposal:
  - Add Security at Transport Level
    - MD5 protocol level security maintained for legacy

Proposed Changes: Transport Security Details

- Options:
  - Separate Port
  - STARTTLS
    - Add new TACACS+ packet Type 0: STARTTLS
    - Client sends as first packet in connection
    - Content of first packet is ClientHello
    - If Server accepts then responds with ServerHello,
    - Handshake then proceeds to upgrade connection.

Proposed Changes: Deprecations

- Remove SENDPASS option (Previously marked deprecated)
- Removed Normative parts of Legacy Elements of protocol:
  - ARAP
  - SendAuth

Open Questions

- Confirm STARTTLS approach vs Separate port for TLS
- Identify whether Authorization and Accounting attributes should be regulated.
  - Proposal: Not to regulate due to overhead.
  - Namespacing (such as Vendor number in RADIUS VSA) would break backwards compatibility

Q&A

Support Slides

Main Features of Protocol

Distinct phases: Authentication, Authorization and Accounting (Types 1-3)

- Essentially three distinct sub-protocols
- Clear separation of Authentication from Authorization enhances main use case for Command Authorization
- TCP permits more reliable Accounting

Main Features of Protocol

- Authentication Flows:
  - Iterative Reply/Continue to cover most requirements
  - Standard Flows covered in RFC, but protocol not limited to these flows
- Authorization/Accounting
  - Attribute based extensibility
  - Free-format AV Pairs of type Mandatory or Optional (Determined by Separator character).

Typical Flow