RFC 6421: Roadmap to Secure RADIUS

Bernard Aboba

History

- Limitations of RADIUS security have been long understood.
  - Security of RFC 2058 (RADIUS Authentication), published in January 1997, described as “barely adequate” during IESG review.
  - As RADIUS usage expanded from dialup networking to VPN and 802.11, additional concerns emerged.
- RFC 3579 (RADIUS/EAP), published in September 2003 describes known attacks and potential solutions.
  - Section 4.3 (Security Issues) is 8 pages long!
    - Includes analysis of security issues (including dictionary and known-plaintext attacks)
    - Describes privacy issues (leaking of geographic location) that emerged in 802.11 use.
  - Section 4.2 specifies RADIUS over IPsec for security services (confidentiality, authentication and replay protection)

Roadmap for Securing RADIUS

- IETF 66 Montreal, July 2006: Security Area Directorate requests RADEXT WG to review security deficiencies and add a work item to the RADEXT WG charter.
- March 2008: David Nelson submits draft-nelson-radext-crypto-agility-requirements-00
- November 2011: RFC 6421 (Crypto-agility Requirements for RADIUS) published.
  - Summarizes state of RADIUS security
  - Describes crypto-agility requirements
  - Lays out a two-stage process for standardization of Secure RADIUS
    - Stage 1: Publication of experimental RFCs
    - Stage 2: Promotion of proposal(s) to the Standards Track.

RFC 6421: Crypto-Agility Requirements

- Section 1.3: Standards Track Publication Requirements
  - Evaluation against requirements.
  - Summary of deployment experience.
  - Evidence of multiple interoperable implementations.
- Section 2: Definition of crypto-agility
  - “Ability of a protocol to adapt to evolving cryptography and security requirements.”
  - “Negotiation of cryptographic algorithms MAY occur within the RADIUS protocol, or within a lower layer such as the transport layer.”
    - Proposals focused on the transport layer approach using (D)TLS.
  - “Proposals MUST NOT introduce generic new capability negotiation features into the RADIUS protocol or require changes to the RADIUS operational model.”
    - “A proposal should focus on the crypto-agility problem and nothing else”
    - “Proposals SHOULD NOT require new attribute formats”.
- Section 3: Current state of RADIUS security

RFC 6421 Crypto-Agility Requirements (cont'd)

- Section 4.2 (Security Services):
  - MUSTs: per-packet integrity and authentication, per-packet replay detection, cryptographic algorithms deemed "acceptable" by NIST with no deprecation date, strong & fresh session keys
  - RECOMMENDED: confidentiality, support for X.509 certificates, pre-shared keys.
  - OPTIONAL: encryption and E2E security of individual RADIUS attributes.
- Section 4.3 (Backward Compatibility)
  - An implementation that supports both crypto-agility and legacy mechanisms MUST be able to talk with legacy RADIUS clients and servers (using the legacy mechanisms).
    - Proposals met requirement by using a separate port.
- Section 4.4 (Interoperability and Change Control)
  - MUSTs: IETF change control, interoperability between independent implementations.
- Section 4.6 (Automated Key Management)
  - AKM is RECOMMENDED for RADIUS and REQUIRED for cryptographic modes of operation requiring frequent key changes.
    - Proposals met requirement via (D)TLS.

Documents Published as Experimental

- RFC 6614: TLS Encryption for RADIUS, published May 2012
  - Section 1: Use in roaming networks such as eduroam
  - Section 1.3: Open questions
    - Certificate verification options
    - TLS-PSK configuration
  - Section 2.1: Use of TCP port 2083
  - Section 2.3: Connection setup
    - Support for TLS 1.1/1.2
    - Required ciphersuites
    - PKI support required, TLS-PSK support optional, certificate fingerprint support optional
  - Section 2.4: Connecting client identity
  - Section 2.5: single TCP port for all packet types
  - Section 3: Informative: design decisions
  - Section 4: Compatibility with other transports
  - Section 5: IANA Considerations
  - Section 6: Security Considerations
    - Confidentiality required.

Documents Published as Experimental (cont'd)

- RFC 7360: RADIUS over DTLS, published September 2014
  - Section 1: Issues encountered in RADIUS over IPsec
  - Section 2.1: Changes to RADIUS
    - "Requires that RADIUS remain largely unchanged to ensure the simplest possible implementation and widest interoperability"
  - Section 3.2 Server Behavior, Section 4 Client Behavior
    - Includes ciphersuite requirements
  - Section 6: Implementation Guidelines
    - Support for both TLS-PSK and PKI authentication
  - Section 8: IANA considerations
    - Allocation of UDP port 2083.
  - Section 9: Implementation status (radsecproxy & jradius)

What Happened Next…

- 16+ years since the IETF Security Area first initiated work on RADIUS crypto-agility.
- Concerns relating to RADIUS privacy and security issues have grown.
  - Shared secret cracking increasingly feasible.
  - Location APIs have magnified impact of location leaks.
- Experimental proposals have been in the field for 8-10 years.
  - Some implementation and deployment experience.
  - Limited market penetration. Why?
    - PKI operational issues?
    - Gaps in TLS-PSK specification?
    - Limitations of open source libraries?
    - Lack of a testing and certification process (e.g. WFA)

Where Do We Go From Here?

- Time to move ahead on Phase 2 of the RFC 6421 process.
- Replacing a core element of the Internet architecture will take time.
  - Secure RADIUS (SRADIUS) not a complex patch (2000 lines), but vendors likely to make it available only on new devices.
  - Mixed deployments (legacy RADIUS and SRADIUS) likely to persist until all legacy clients are retired.
- Need to get device vendors on board
  - Address implementation, interop and deployment blockers.
    - Support for TLS-PSK?
  - May require updates to open source libraries.
  - Cooperation with industry for test and certification.
  - Reference deployments to establish credibility.
- RADIUS deprecation the final (not initial) step.
  - Needs to be coordinated with standards track publication.