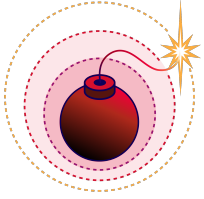
RADIUS/UDP Considered Harmful

Sharon Goldberg, Miro Haller, **Nadia Heninger**, Mike Milano, Dan Shumow, Marc Stevens, and Adam Suhl

July 25, 2024



Academic publication

RADIUS/UDP Considered Harmful
Sharon Goldberg, Miro Haller, Nadia Heninger, Mike Milano, Dan Shumow, Marc Stevens, and Adam Suhl.
To appear at USENIX Security, August 2024.

`https://www.blastradius.fail`

Attack summary

Protocol vulnerability: RADIUS hard codes weak authentication based on broken MD5 hash function.

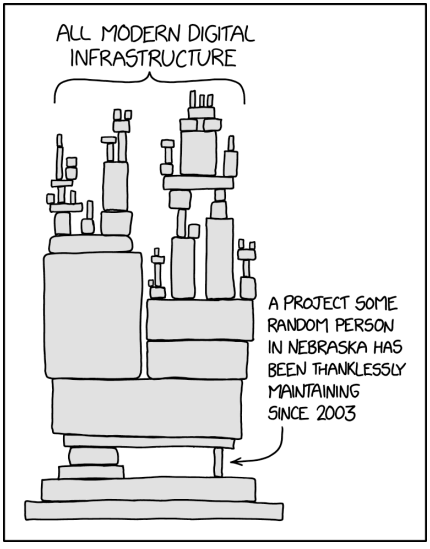
A man-in-the-middle network attacker can forge arbitrary RADIUS responses for non-EAP authentication modes.

- For example can turn an Access-Reject into an Access-Accept.
- Can add arbitrary network access attributes to Access-Accept.
- etc.

Attack is practical.

Vulnerability present from earliest versions of RADIUS in 1994; never updated.

Obligatory XKCD



- RADIUS is the de facto standard lightweight protocol for authentication, authorization, and accounting (AAA) for networked devices
- RADIUS is *everywhere*: ISPs (DSL/FTTH), 802.1X, WiFi, mobile roaming, IoT, router admin access…

RADIUS protocol sketch

RADIUS Access-Request

`User-Name=username; User-Password=Mjg2NzU1Z...`

RADIUS Access-Accept

RADIUS client

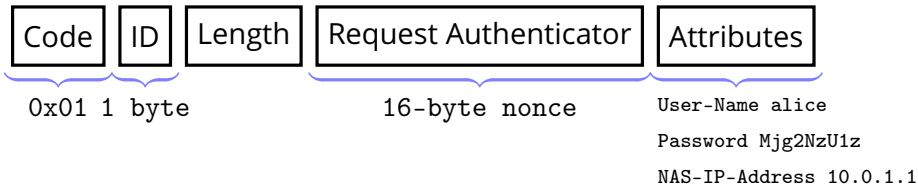
RADIUS server

- RADIUS requests, responses often sent over UDP
- RFC 6614 TLS Encryption for RADIUS (2012) never left experimental status.
- `draft-ietf-radext-radiusdtls-bis` (D)TLS Encryption for RADIUS

Apologies to XKCD

RADIUS Packet Formats

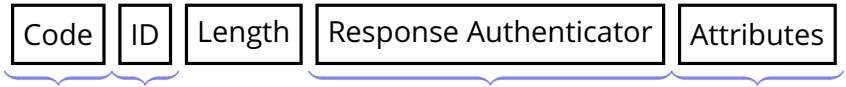
Access-Request



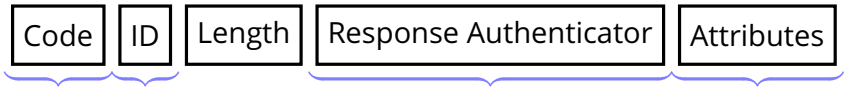
- Access-Request packet contents unauthenticated.
- Source IP address is used to identify/validate client.
- Client and server share fixed shared secret.
- Passwords obfuscated using MD5+shared secret.

RADIUS Packet Formats

Access-Accept



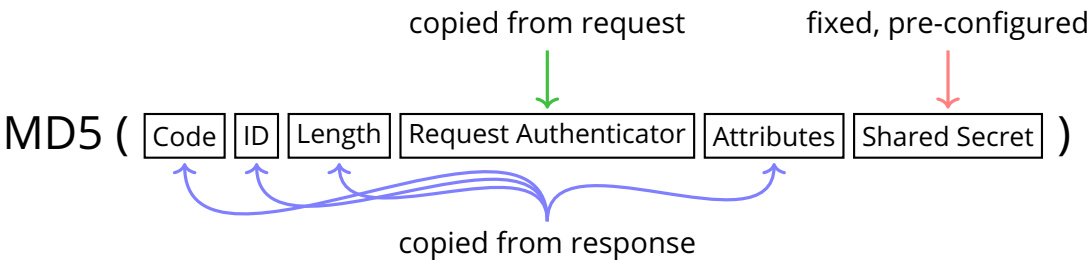
Access-Reject



- Responses authenticated with ad hoc `Response Authenticator` MD5 hash.

RADIUS Response Authenticator

The Response Authenticator is computed as



RADIUS/MD5 History

1991 RADIUS initially designed by Livingston.

1993 Known weaknesses in MD5.

1994 Initial RADIUS IETF draft hard codes ad hoc MD5 construction.

1995 SHA-1 published.

1996 HMAC published.

1997 RADIUS RFC 2058 published with ad hoc MD5 construction.

2000 RADIUS Extensions RFC 2869 defines optional Message-Authenticator HMAC-MD5 attribute.

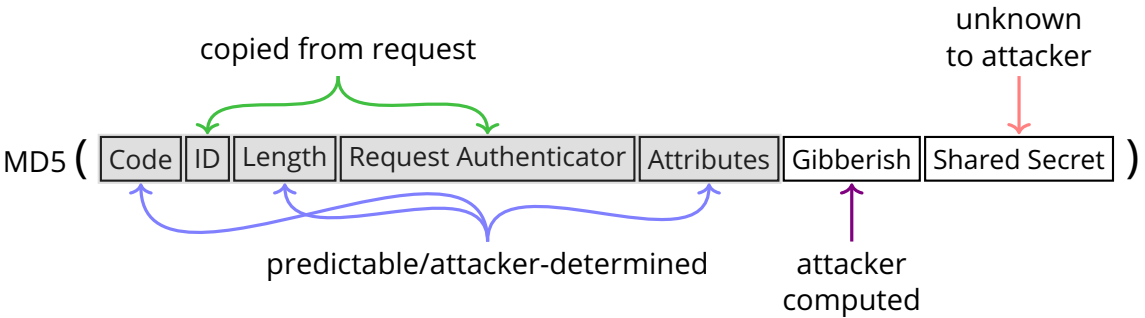
2004 First full MD5 collision.

2007 MD5 chosen-prefix collision.

2007 RFC 5080 Message-Authenticator remains optional.

2023 `draft-ietf-radext-deprecating-radius-00` “there have been (as yet) no attacks on RADIUS Authenticator signatures which are stronger than brute-force”.

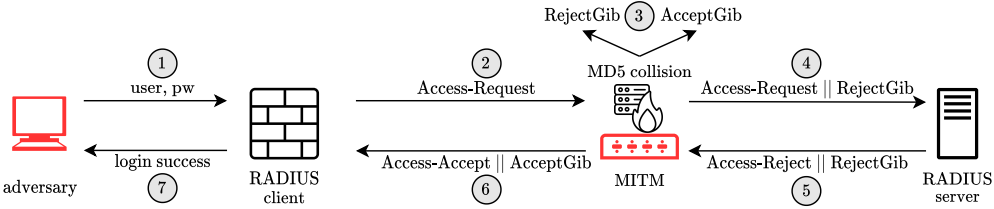
Chosen-Prefix MD5 Collisions against Response Authenticator



1. Response Authenticator vulnerable to MD5 chosen-prefix attack.
2. MITM attacker injects collision gibberish into `Proxy-State` attribute.
3. Attacker copies valid `Response Authenticator` from observed response to desired forged response.

Attack summary

More details to be presented tomorrow in radext meeting.



1. Adversary logs into victim NAS with invalid password.
2. Victim NAS makes RADIUS Access-Request to RADIUS server.
3. MITM intercepts request and computes MD5 collision.
4. MITM injects collision gibberish into Proxy-State attribute in request.
5. Victim RADIUS server rejects request.
6. MITM copies Response Authenticator from reject into forged Access-Accept.
7. Victim NAS RADIUS client receives forged accept and permits login.

Mitigating factors and complications

- Attack requires full man-in-the-middle network access.

  Management VLAN less vulnerable; UDP over open internet more vulnerable.

- The `Message-Authenticator` attribute is HMAC-MD5 and is *not* vulnerable to MD5 collision.

  This attribute is *optional* and not historically required except for EAP.
  $\implies$ EAP authentication modes not vulnerable to practical attack.

Short-term mitigation: `draft-ietf-radext-deprecating-radius-02` All requests and responses should include and verify `Message-Authenticator` attribute.

Long-term mitigation: `draft-ietf-radext-radiusdtls-bis-02` All RADIUS traffic should be encapsulated in (D)TLS tunnel.

Discussion

Analogy to SSL/TLS attacks: worries over 3 years of backwards compatibility in 1990s led to 30 years of insecurity.

- How did this go unnoticed for so long?
- How do we find other neglected insecure protocols/constructions?

- Smoothest vulnerability disclosure I've done; shout out to CERT and Alan.