The RADIUS protocol, widely used for network access authentication, faces significant vulnerabilities due to its reliance on MD5 hashing and UDP. MD5, once a trusted crypto. The RADIUS protocol, widely used for network authentication, is increasingly vulnerable due to its reliance on MD5 hashing and UDP. While RADIUS has been a backbone for network access control, its use of MD5—a cryptographic hash function known for its now-outdated security—has created significant security risks. In combination with UDP, which is inherently less secure than TCP, attackers have a pathway to exploit weaknesses in both encryption and data transmission.

MD5's vulnerability lies primarily in its susceptibility to hash collisions and replay attacks. A hash collision occurs when two different sets of data produce the same hash output. This undermines the uniqueness that hashing algorithms are meant to provide, allowing an attacker to craft malicious input that mimics a legitimate one, potentially bypassing security checks. In the context of RADIUS, this means that attackers could forge authentication credentials or manipulate packet data in ways that the server might accept as valid, compromising the integrity of the authentication process.

A replay attack is another serious threat when using MD5 in RADIUS over UDP. Since UDP is stateless, it lacks the built-in mechanisms to prevent an attacker from capturing and reusing legitimate packets to gain unauthorized access. By capturing authentication data during transmission, an attacker can resend (or "replay") that data later to impersonate a legitimate user. The Cloudflare blog outlines how this type of attack is particularly effective in UDP environments, where session tracking is minimal, and the weaknesses in MD5 make it even easier to exploit these interactions.

To mitigate these vulnerabilities, security experts strongly recommend transitioning from MD5 to stronger cryptographic algorithms like SHA-256. Modern algorithms are designed to be collision-resistant and better equipped to handle the evolving landscape of attacks. Additionally, moving RADIUS communications from UDP to TCP can enhance security by incorporating connection-based verification, which mitigates the risks of replay attacks. Alternatively, Rublon suggests using IPsec to encrypt and authenticate communication between RADIUS clients and servers, further reducing the risk of interception or tampering.

Authors, R. (2024, July 16). *Blast-radius attack: Radius/UDP and MD5 authentication*. https://rublon.com/blog/blast-radius-udp-md5-vulnerabilities-mitigation-strategies/

Sharon GoldbergMiro Haller (Guest Author)Nadia Heninger (Guest Author)Michael Milano (Guest Author)Dan Shumow (Guest Author)Marc Stevens (Guest Author)Adam Suhl (Guest Author), Goldberg, S., Author), M. H. (Guest, Author), N. H. (Guest, Author), M. M. (Guest, Author), D. S. (Guest, Author), M. S. (Guest, Author), A. S. (Guest, Prince, M., Graham-Cumming, J., Tremante, M., One, C., Martinho, C., Chen, M., Hall, D., & Keane, M. (2024, October 9). *Radius/UDP vulnerable to improved MD5 collision attack*. The Cloudflare Blog. https://blog.cloudflare.com/radius-udp-vulnerable-md5-attack/