A History

ALAN DEKOK - SAAG - IETF 120
LET’S RECAP

- 1991 - RADIUS defined by Livingston
- 1997 - RFC 2038, after some discussion with the IESG on security
- 1998 - HMAC auth starts being defined
- 2000 - RFC 2869 says “authenticated packets aren’t necessary”
- 2007 - RFC 5080 - Please can we just use HMAC? \(^\text{No.}\)
- 2024 - Oops. Maybe we should have fixed this a while ago.
THE PUSH-BACK

‣ Does anyone still use RADIUS?
‣ Hasn’t it been replaced by Diameter?
‣ But hasn’t everyone switched to EAP / EAP-TLS?
‣ But surely no one is using PAP / CHAP / MS-CHAP over RADIUS/UDP, right?
‣ But we can use Kerberos, or TACACS+ or IPSec, right?
IS THERE ANYTHING SIMILAR?

› CVE-2024-3661

› a local DHCP server can spoof routes and get some VPNs to bypass the VPN. The underlying issue has been known for decades. Paul has opinions here.


› State-sponsored actors monitor SS7 / Diameter to track individuals, and attack them

› They don't mention RADIUS, likely because no one pays attention to it

› https://www.akamai.com/blog/security-research/spoofing-dns-by-abusing-dhcp

› DHCP can request DDNS updates, leading to unauthenticated arbitrary DNS record overwrite

› DNS has been updated with DNS over TLS and DNS over HTTPS, so that's nice.
HOW DID WE GET HERE?

‣ Operational people don’t always talk to crypto people
  ❖ and vice versa

‣ Unless the specs are extremely clear on security issues, they will get ignored

‣ Even for 802.1X, we use post-quantum crypto, 4096-bit keys, and then...
  ❖ raw UDP packets with no authentication or integrity checks

‣ Maybe we can do better?
WHAT TO DO NEXT?

‣ Something? Anything?

‣ Who’s responsible, other than the IETF?