Deprecate All The Things

ALAN DEKOK - RADEXT - IETF 120
IT’S BEEN AN INTERESTING FEW MONTHS

‣ The BlastRADIUS attack means that the doc had to be substantially changed
  ‣ Description of the attack, mitigations, etc.
  ‣ Upgrade everything.
  ‣ Or not. It’s fine, right?
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?
‣ 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› Hasn’t it been replaced by Diameter?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?
› The attack is hard, so I don’t need to upgrade, right?
REITERATING RECOMMENDATIONS

- Focus extended from just UDP/TCP to any insecure practice
- Substantial text added about MS-CHAP
  - We should consider MS-CHAP to be 100% broken.
- Text on PAP vs CHAP and password storage
  - Most public recommendations are horrifically wrong
  - PAP is secure.
LAST MINUTE NOTES

› Nothing recommends delaying Access-Rejects

› It can help with dictionary attacks

› Nothing recommends constant-time comparisons

› for Message-Authenticator or Response Authenticator
QUESTIONS?

‣ Why has no one looked at this in the past 25 years?