Deprecating insecure practices

LET’S JUST BE SECURE
ALAN DEKOK IETF 118
DEPREDATE INSECURE PRACTICES

› The document seems close(r) to being done
› Should perhaps be published after 6614bis
› Are we prepared to wait that long?
› Do we close off this document, and push on 6614bis?
CHANGES SINCE IETF 117

‣ Focus extended from just UDP/TCP to any insecure practice

‣ Much text 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
PROPOSAL

- Has been accepted as a WG document
- Let’s put it on hold as mostly done, and focus on 6614bis