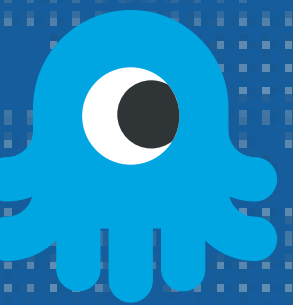


Deprecating insecure practices

LET'S JUST BE SECURE

ALAN DEKOK IETF 119



DEPRECATE INSECURE PRACTICES

- ▶ The document seems close(r) to being done
- ▶ Should perhaps be published along with TLSbis
- ▶ MD5 is only getting worse over time



CHANGES SINCE IETF 117

- ▶ 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



PROPOSAL

- ▶ Has been accepted as a WG document
- ▶ Mostly in last call, just waiting for some updates
- ▶ Once finalized, we should publish TLSbis and this document together
- ▶ The document has received substantial reviews
 - ▶ and follows recommended practices going back years

