InkBridge Networks

Blastradius

ALAN DEKOK - EMU - IETF 120

BLASTRADIUS

- Oh boy… 30+ year-old design flaw in RADIUS.
- Does NOT impact EAP. EAP methods over RADIUS are safe.
- What can we learn from this?
  - Ad hoc crypto methods are bad. Very bad.
- Pretty much no one looks at foundational network protocols

THE ATTACK IS REAL, AND A THREAT

- It’s not just theoretical, it’s practical
- The fast MD5 code is publicly available.
- Maybe a few $100 of cloud computing can do the attack in <10s
- An attacker can redirect all ISP subscriber traffic to any domain they want
  - then launch a malware attack on the user

THE INTERNET IS BUILT ON SAND

- Most of the lower-level protocols are insecure, unauthenticated
- We need ways to securely authenticate the user to the network, and the network to the user
- Perhaps leverage EAP to securing more of the network