Addressing the Amplification Vulnerability in Forking Proxies

draft-ietf-sip-fork-loop-fix-00

Robert Sparks
Estacado Systems
What the draft says

• Describes the problem
• Specifies normative fix:
  – IF (and only if) a proxy forks a request, it
    • MUST verify it’s not in a loop
    • SHOULD use loop-detection from 3261
Is simple loop-detection enough?

- Short term - yes - much better than without
- Long term - probably not
  - Same attack over M Aors reduces to generation of $O(2^M)$ requests. Simple mod yields $M^M$.
  - Anything that makes generation of a retargetable URI easier can be leveraged for this type of attack.
    - GRUU
    - Any parameters added to an AOR that would defeat loop detection
What the draft doesn’t discuss

• Limiting the number of concurrently active branches (see max-breadth)
• Additional restrictions on 3rd-party registrations
  – Outbound
  – Consent
Recommended Next Steps

• WGLC/Publish this draft at current scope (loop detection only)
• Continue discussions on other potential improvements as separate efforts