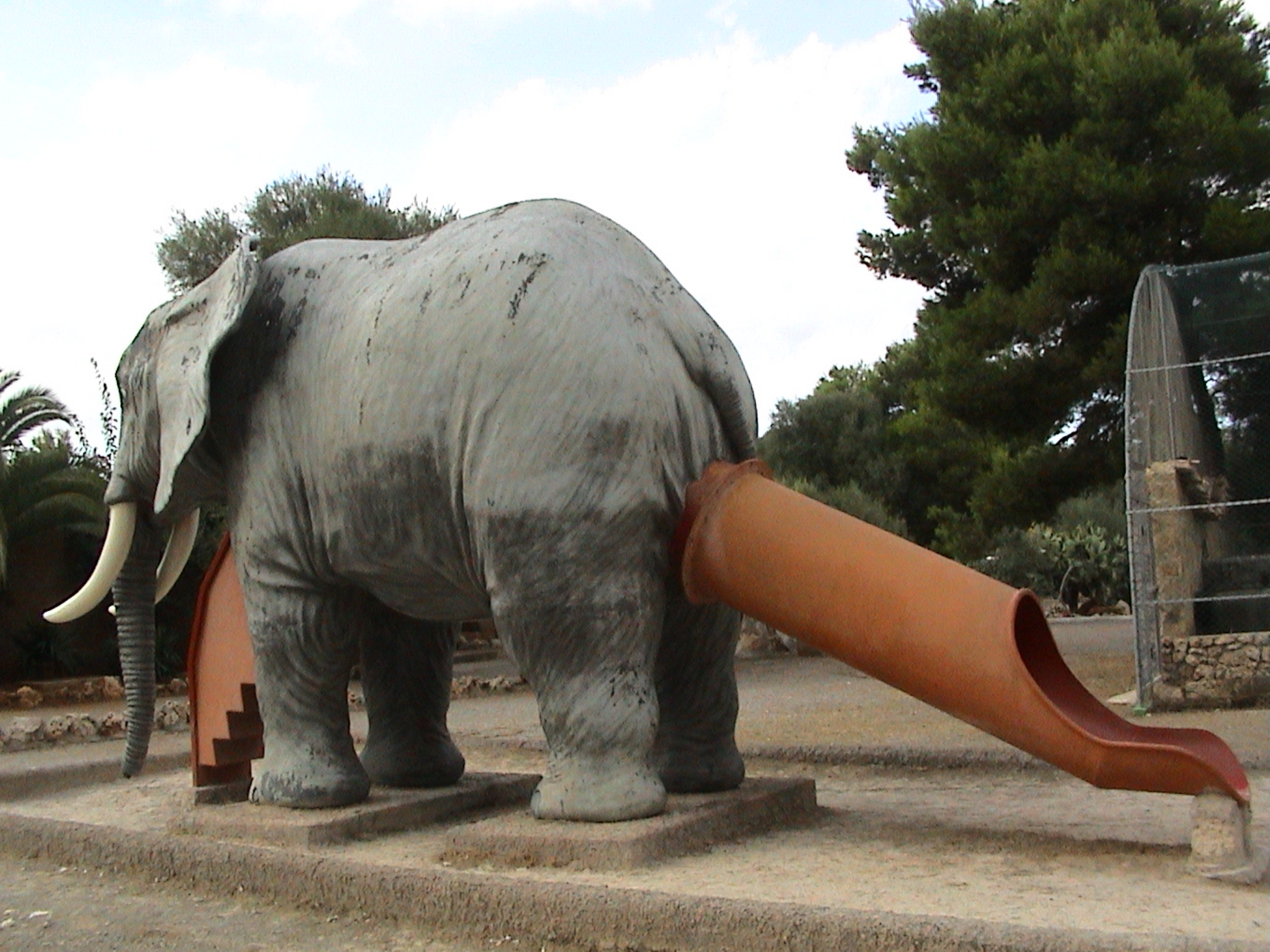
Via Cookies

draft-zourzouvillys-via-cookie-02

IETF 74

theo@voip.co.uk



The Problem

- Amplicifaction of 1:11
- No tracability
- Victim does not need to be a SIP element

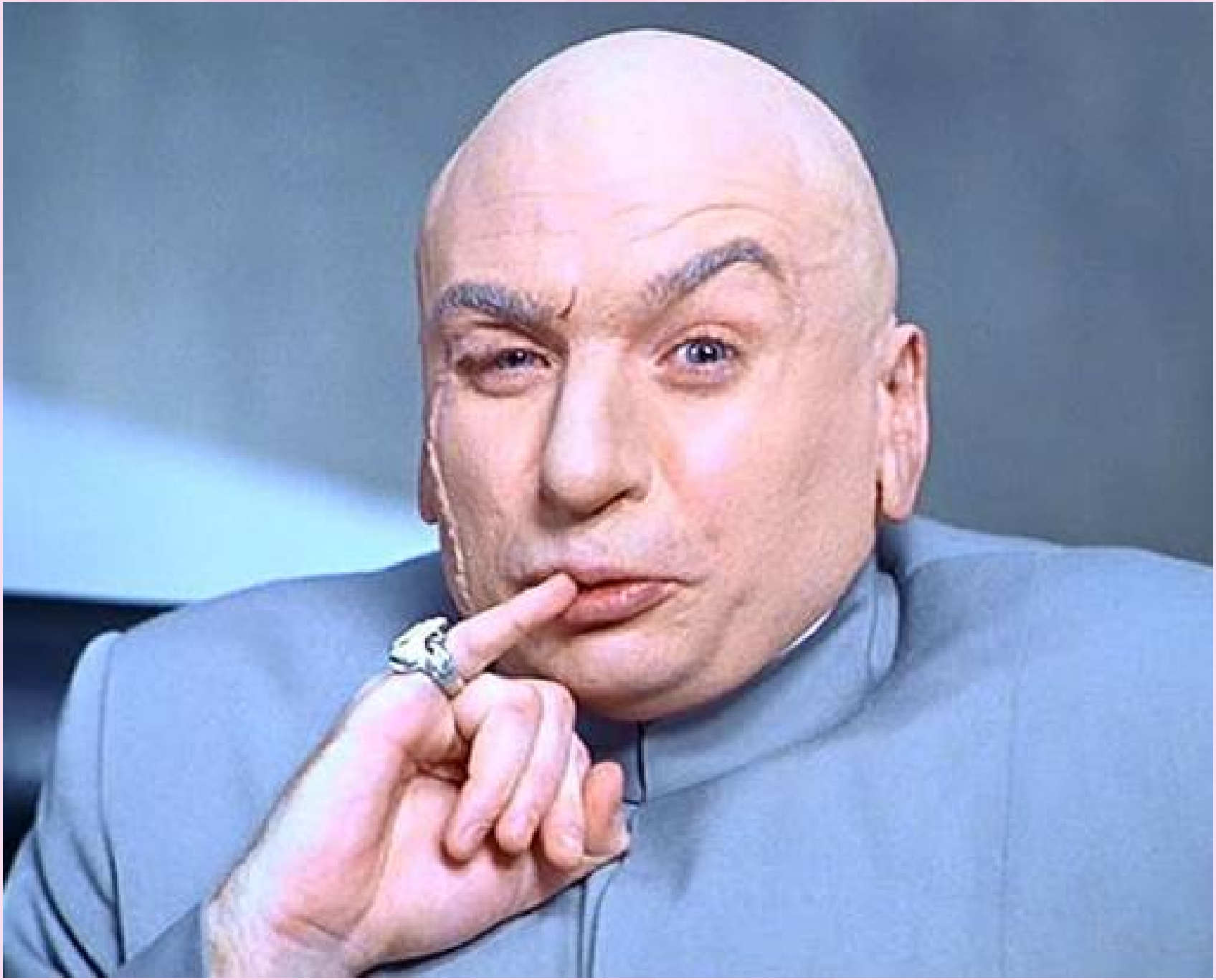
Bang bang bang

INVITE sip:invalid.domain
IP src: 192.0.2.200
IP dst: 192.0.2.1

Atlanta
192.0.2.1

404 Not Found
IP src: 192.0.2.1
IP dst: 192.0.2.200

192.0.2.200



How bad is it
in the real world?

bad

How bad is it?

- last week there were 8.4 million publicly accessible SIP elements on port 5060 UDP.
- 96% of them sent a 4xx response to an INVITE statefully
  - almost all even for stuff that doesn't need to, like malformed SDP
- only 2% are sending non-2xx responses statelessly
- Many hosting companies and DSL providers still don't uRPF
  - will give (real)cookies to anyone who adds, but need slap first
  - still leaves SIDR style problems
- Can walk e164.arpa to find URIs which may return 2xx
- Voicemail and IVR servers are particularly attractive

om nom nom

The (hop by hop) Solution

Other Solutions

- Deprecate UDP
- Anonymous authentication (or even better, null-auth with a nonce addition)
- Walled gardens only
- Pack up and go home (i've always wanted run a farm)

Downsides

- Stateless proxies will need to round-trip them
  - Only affects Outbound stateless proxies with next-hop over UDP

Other Related Problems

- In-Dialog Targeting
- *Voice Hammer* attack, see **draft-rosenberg-mmusic-rtp-denialofservice-00**

Outstanding Issues

- None?

Questions?