Fork Loop Fix
(Take 2)

SIP WG - IETF69
draft-ietf-sip-fork-loop-fix-05
draft-sparks-sipping-max-breadth-01

Robert Sparks
Estacado Systems

SECDIR review found a problem

- Loop detection doesn't mitigate the attack when the attacker uses a larger number of resources
  - Effective with 10s of resources
  - Easy to obtain such resources in the wild
  - Paths through the attack without loops exist with length up to the number of resources
  - Total traffic in the attack with n resources is bounded below by n! messages (see the max-breadth draft)

SECDIR review found a problem

- Attack doesn't affect only the systems providing forking
  - Each participating resource can be configured to fork to a victim as well as each of the other participating resources, flooding that victim with traffic (for this presentation, call this endpoint victim A)

Proposed solution

- Limit the number of messages the attack can produce
- Operates independently from Max-Forwards
- Option 1 (currently what max-breadth says)
  - Limit the number of messages that can be in flight at any given time, but don't change the total number of messages that might play out
- Option 2 (called out as an open issue)
  - Limit the number of messages that can be generated period

Option 1 - limiting simultaneous messages

- Spreads out the impact on victim A
  - Improves opportunity for recovery
- Effectively limits propagation rate
  - Allows Timer-C generated CANCELs or final responses from the victim to help stop the attack
- Doesn’t change the overall reach of a request
- Doesn’t prevent forking
  - but may limit it to serial forking as available breadth is committed

Option 2 - limiting the total number of messages

- Don’t allow breadth to be reclaimed as branches complete
- Completely limits the impact on victim A
- Changes the reach of a request into the network

Discussion

- Is this the right direction? (proposal: yes)
- Which of these options do we pursue?
  - Limit the messages in flight due to this request at any given time
  - Limit the total number of messages this request creates

Essential Corrections

SIP WG - IETF69
draft-drage-sip-essential-correction-01

Robert Sparks
Estacado Systems

Tracking what’s in flight

- http://www.softarmor.com/mediawiki/index.php/Essential_Corrections_Tracking

Open question: What’s the format?

- Current plan is for 2 sections in the correction RFC (per drage-sip-essential-correction)
    - Non-normative text motivating/explaining each correction
    - Normative changes made by text like “replace paragraph 2 in section 45.2 with <yaddayadda>”
- -invfix anticipates this format
- 4320 used a similar approach
- Is there something better?