SIP DoS Attack Detection

An Ontological Approach
SIP as the VoIP Control System
SIP Format

SIP Request Message
INVITE sip:happy@193.11.155.123 SIP/2.0
Via: SIP/2.0/UDP 193.11.155.93:5063
To: happy <sip:happy@193.11.155.123>
From: dopey <sip:dopey@193.11.155.93>
Contact: <sip:dopey@193.11.155.93:5061>
Call-ID: 1-3207@127.0.1.1
CSeq: 1 INVITE
Max-Forwards: 70

SIP Response Message
SIP/2.0 200 OK
Via: SIP/2.0/UDP 193.11.155.93;
   SIP/2.0/UDP 127.0.1.1:5061
From: snowwhite <sip:snowwhite@193.11.155.93:5061>
To: sut <sip:princecharming@193.11.155.123:5060>
Call-ID: 785-3206@127.0.1.1
CSeq: 2 INVITE
Contact: <sip:127.0.1.1:5061;transport=UDP>
INVITE bob@proxy2
100 Trying
180 Ringing
200 OK
ACK
Session active
DoS Attacks

• Web Delay
• DNS Delay
• Malformed Message
• Invite Flood
• Amplification
SIP DoS Attack Ontology
Testbed Setup

Amp Attack

DNS Delay Attack
Amplification Attack
DNS Delay Attack
Malformed Message Attack?
Invite flood attack a subset?
Conclusions

• Once we have an ontology, it is easier to distinguish between DoS Attacks, but...

• Creating an ontology that properly captures the attack can be difficult without distinguishing characteristics

• Sometimes, different attacks look very similar without deep packet inspection.