A DoS-Resistant IP Traceback Approach

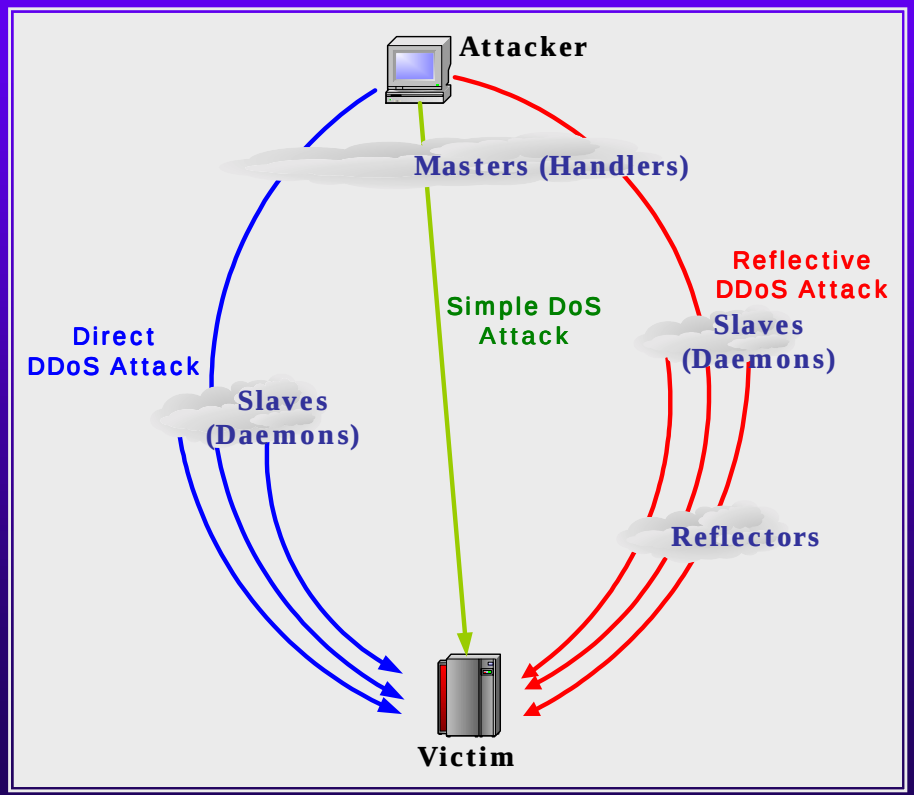
Bao-Tung Wang, Henning Schulzrinne
IRT, Columbia University
Friday, September 12, 2003

Overview

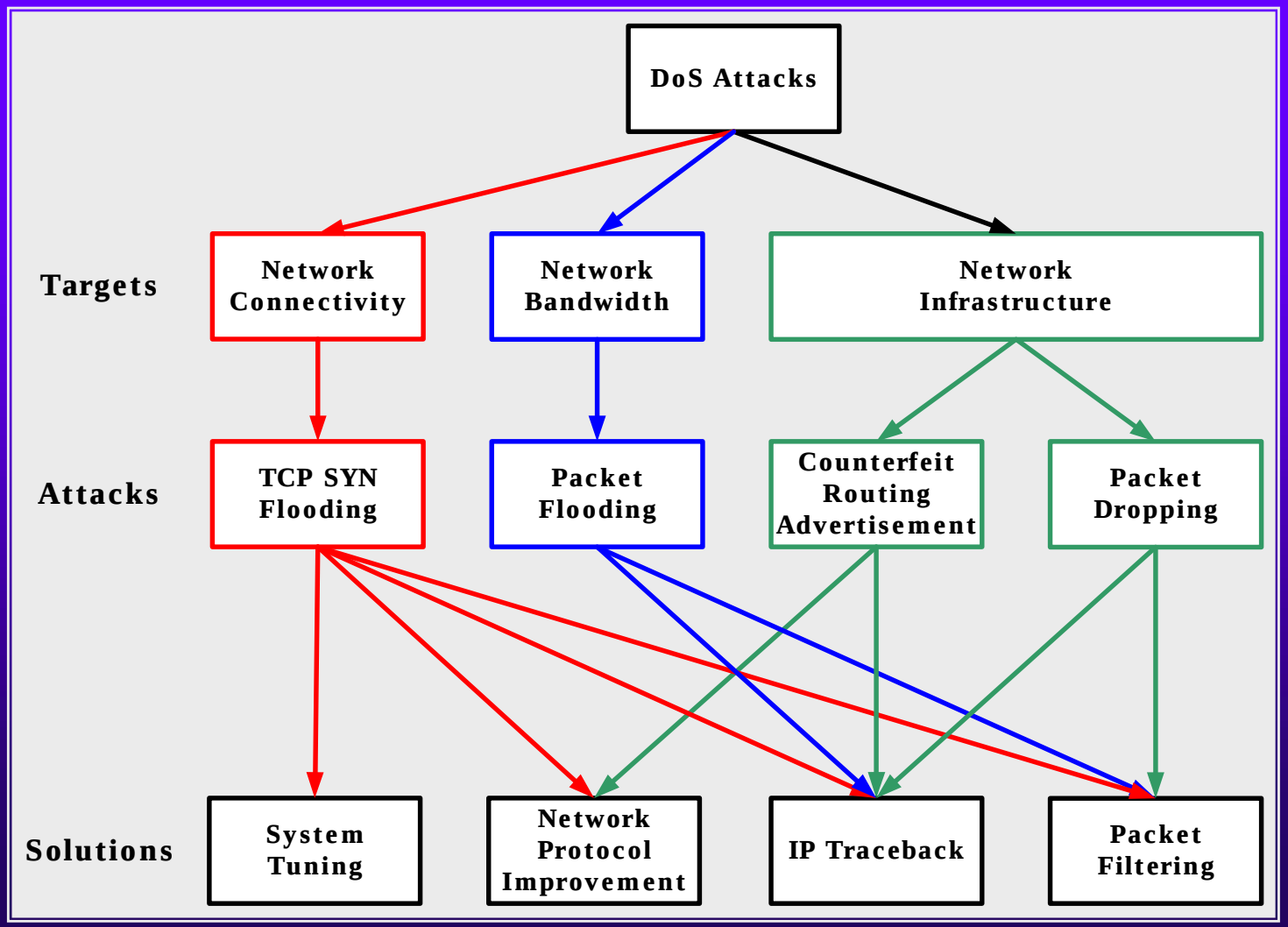
- Definitions
- ICMP Caddie Messages
- IP Traceback Using Caddie Messages
- Evaluations
- Conclusion

Introduction

- DoS (Denial-of-Service)
- DDoS (Distributed DoS) Attacks
  - Direct DDoS
  - Reflective DDoS
- IP Traceback



Proposed Solutions



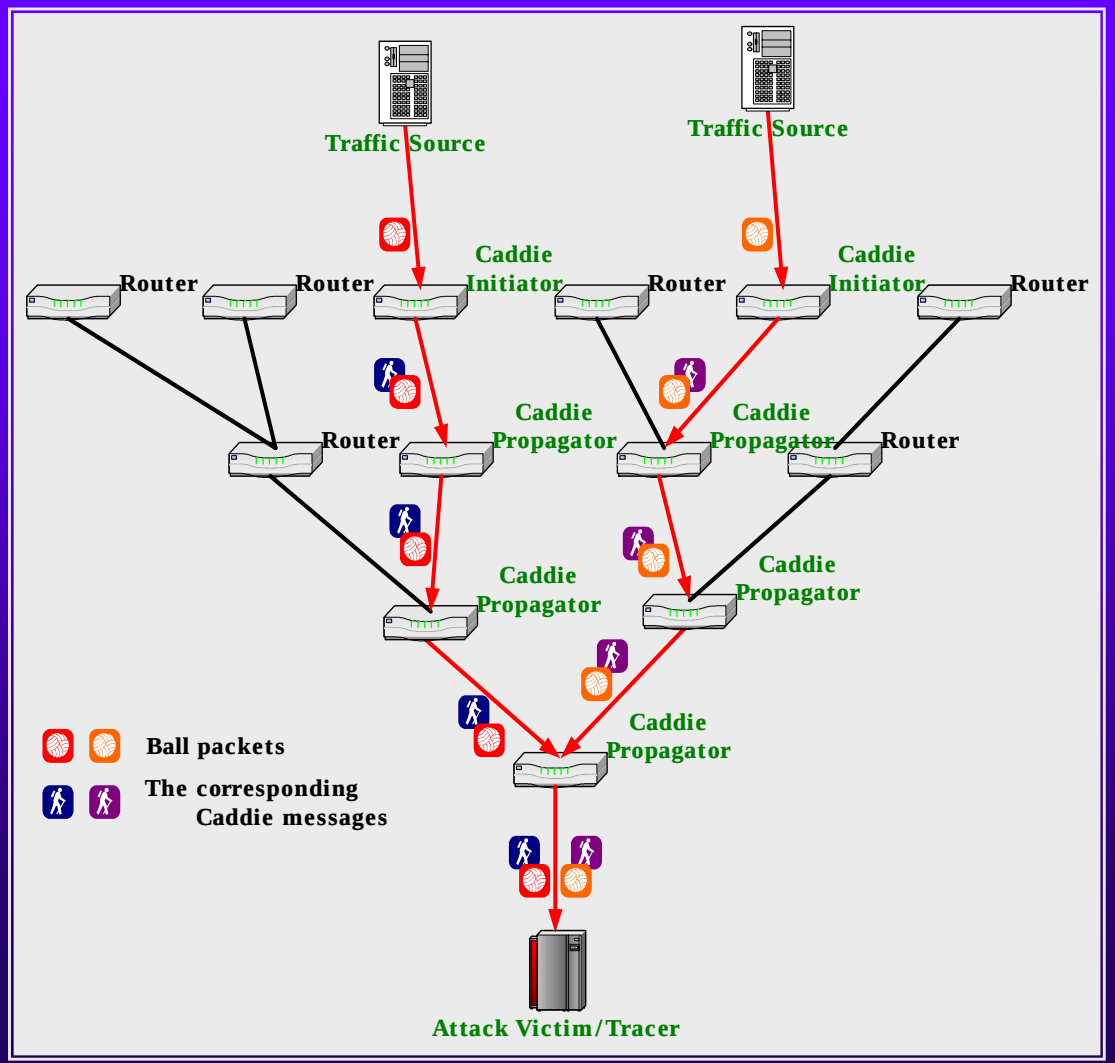
Problems of Existing Solutions

Categories	Examples	Bandwidth Overhead	Storage Overhead	Computation Overhead
Link Testing	**Router Inference**	**Very High**	Low/Low	Low/Low
Logging	**SPIE**	Fair	**Very High**/Low	Fair/Low
Overlaying	**CenterTrack**	**High**	Low /Low	Low /Low
In-Band Marking	**PPM**	None	None/**Very High**	Low/**Very High**
	AAM	None	Low/**High**	Low/**High**
Out-of-Band ICMP Messaging	**iTrace**	**High**	None/**High**	Low/**Very High**
	ID-iTrace	**High**	**High**/Fair	Low/**High**
	iCaddie	Fair	Low/Low	Low /Fair

(A/B indicates the overhead in the network is A and that at the destination is B)

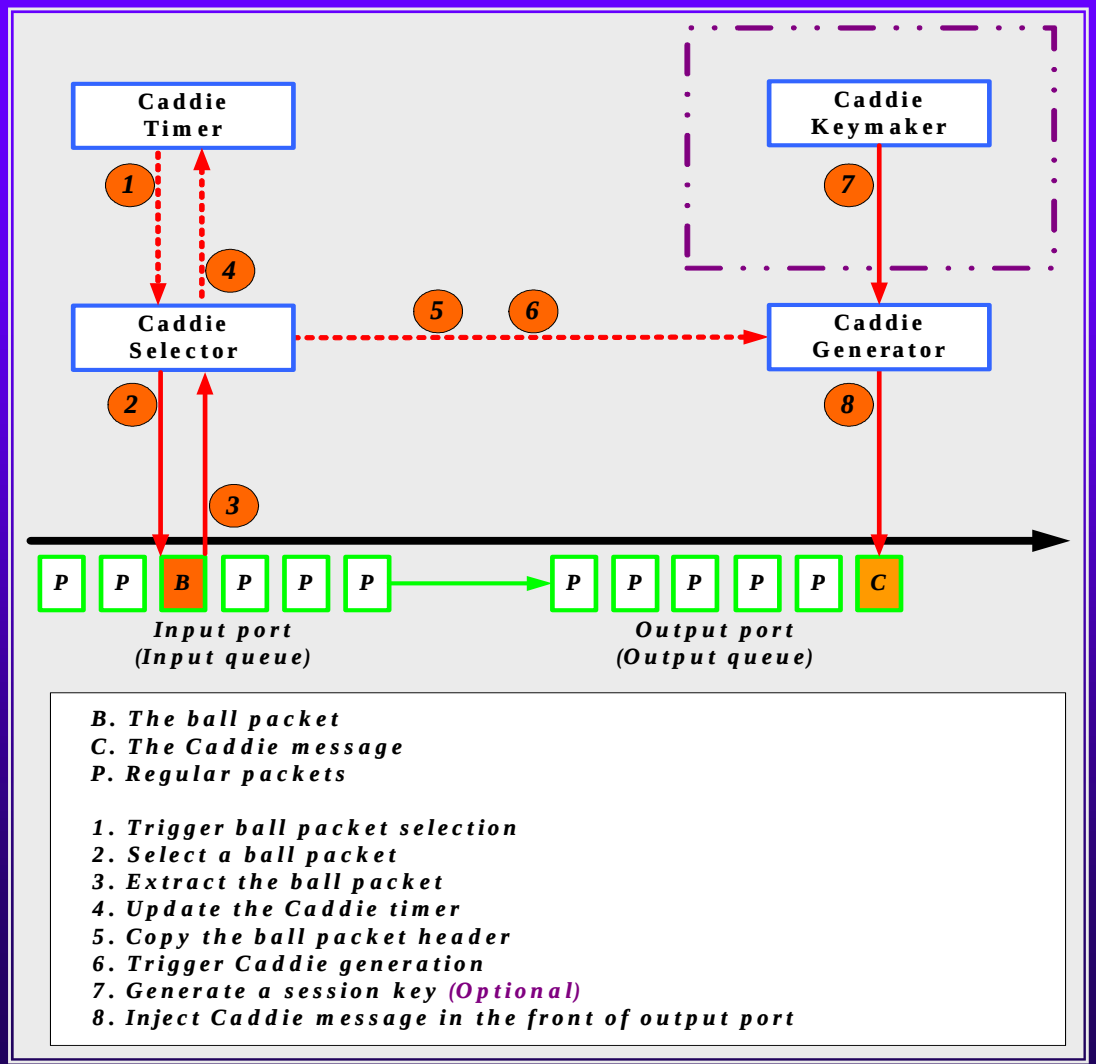
ICMP Caddie Messages

- Ball Packets
- Caddie Messages
- Caddie Initiators
- Caddie Propagators

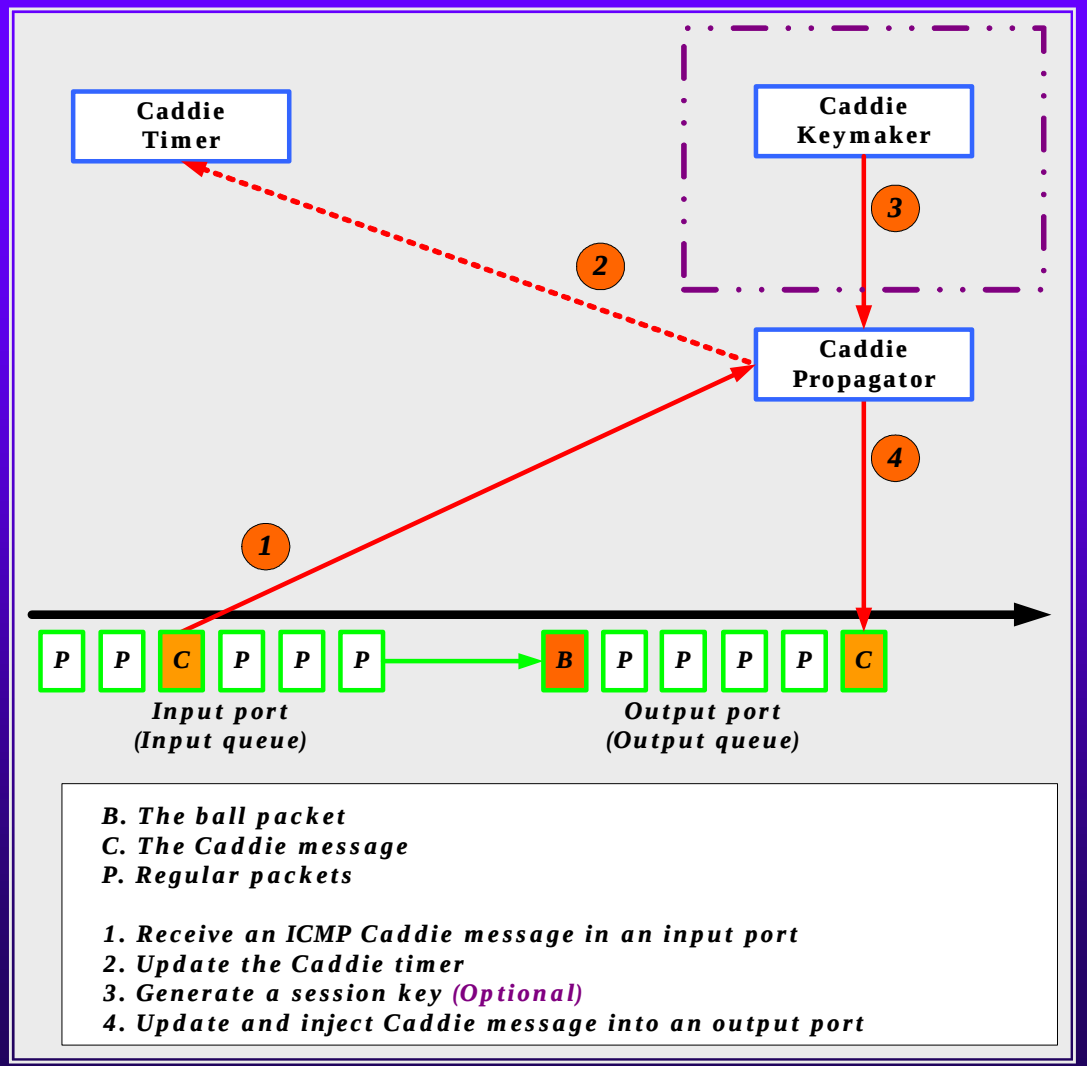


Caddie Message Generation

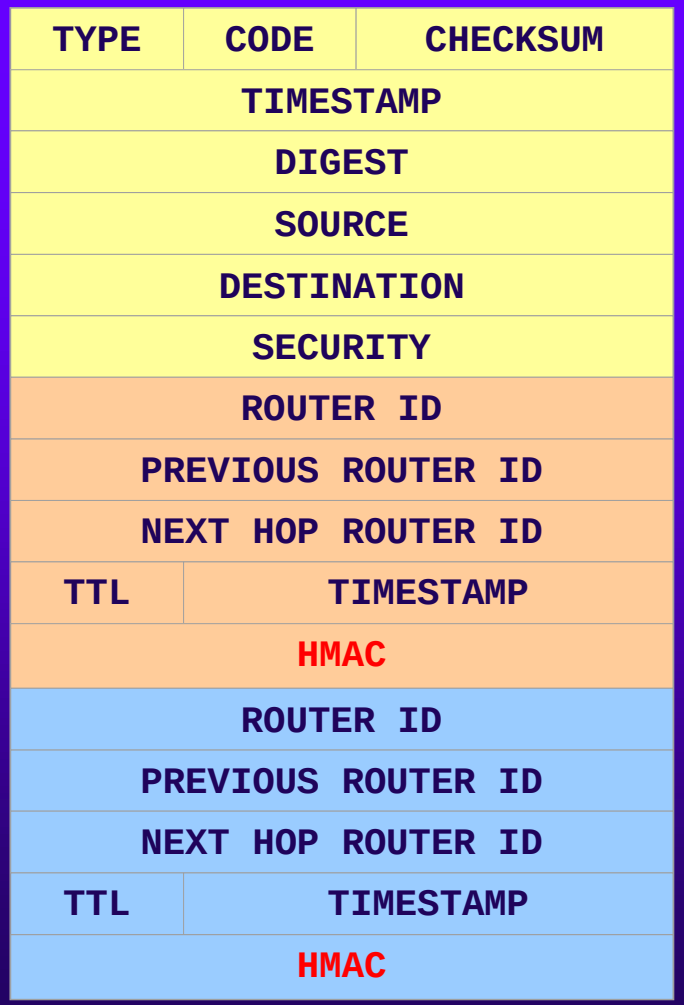
- Caddie Selector
- Caddie Timer
- Caddie KeyMaker



Caddie Message Propagation



A Caddie Message



ICMP message header

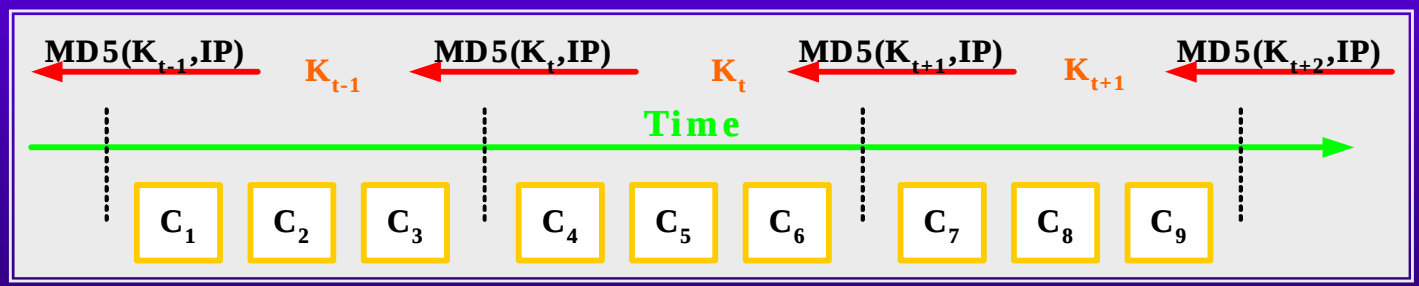
Caddie message header

First element of the ROUTER LIST (by Caddie Initiator)

Successive ROUTER LIST elements (by Caddie Propagators)

Time-Release Key Chain (TRKC)

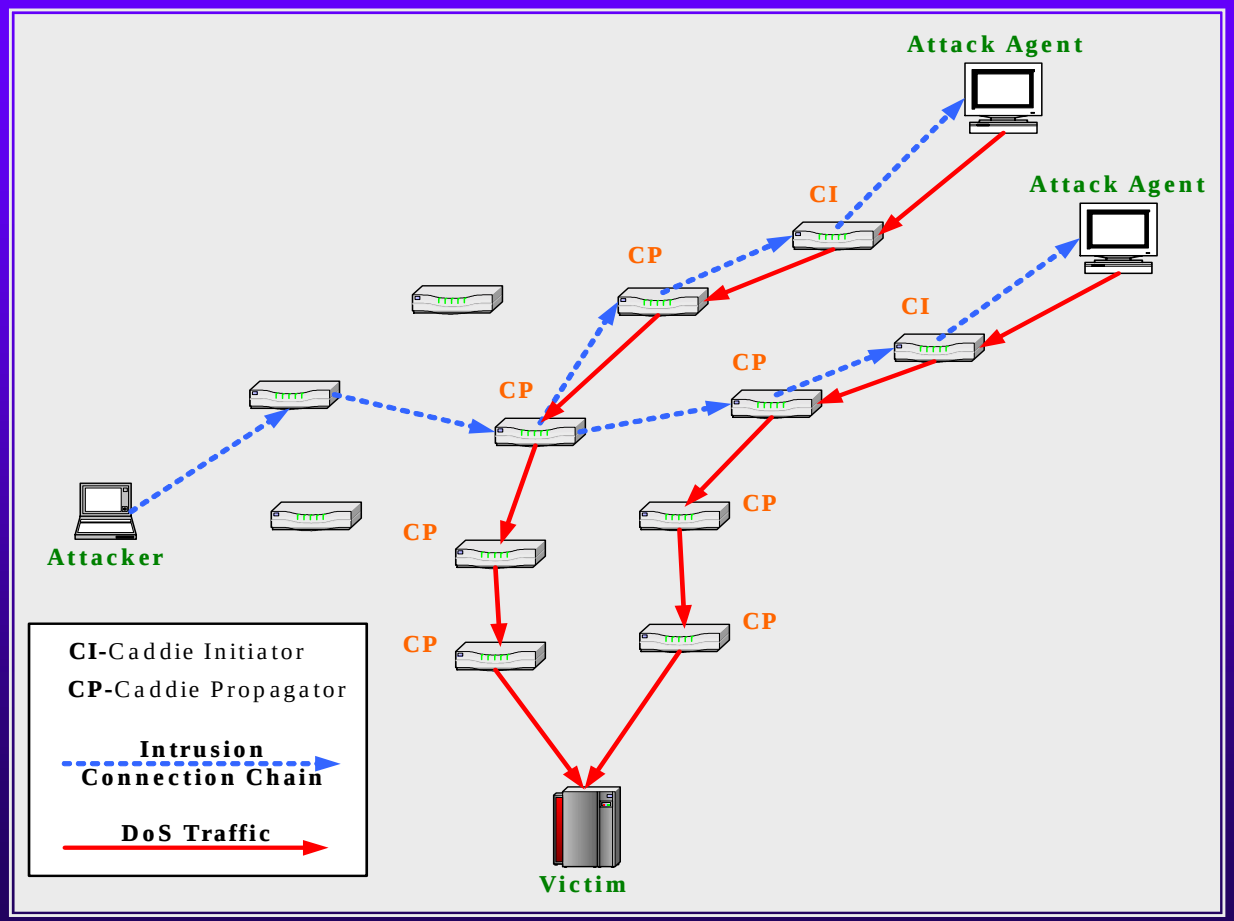
- Key Generation
- HMAC Calculation
- Caddie Message Authentication



C_i: Caddie Messages
K_t: Session keys

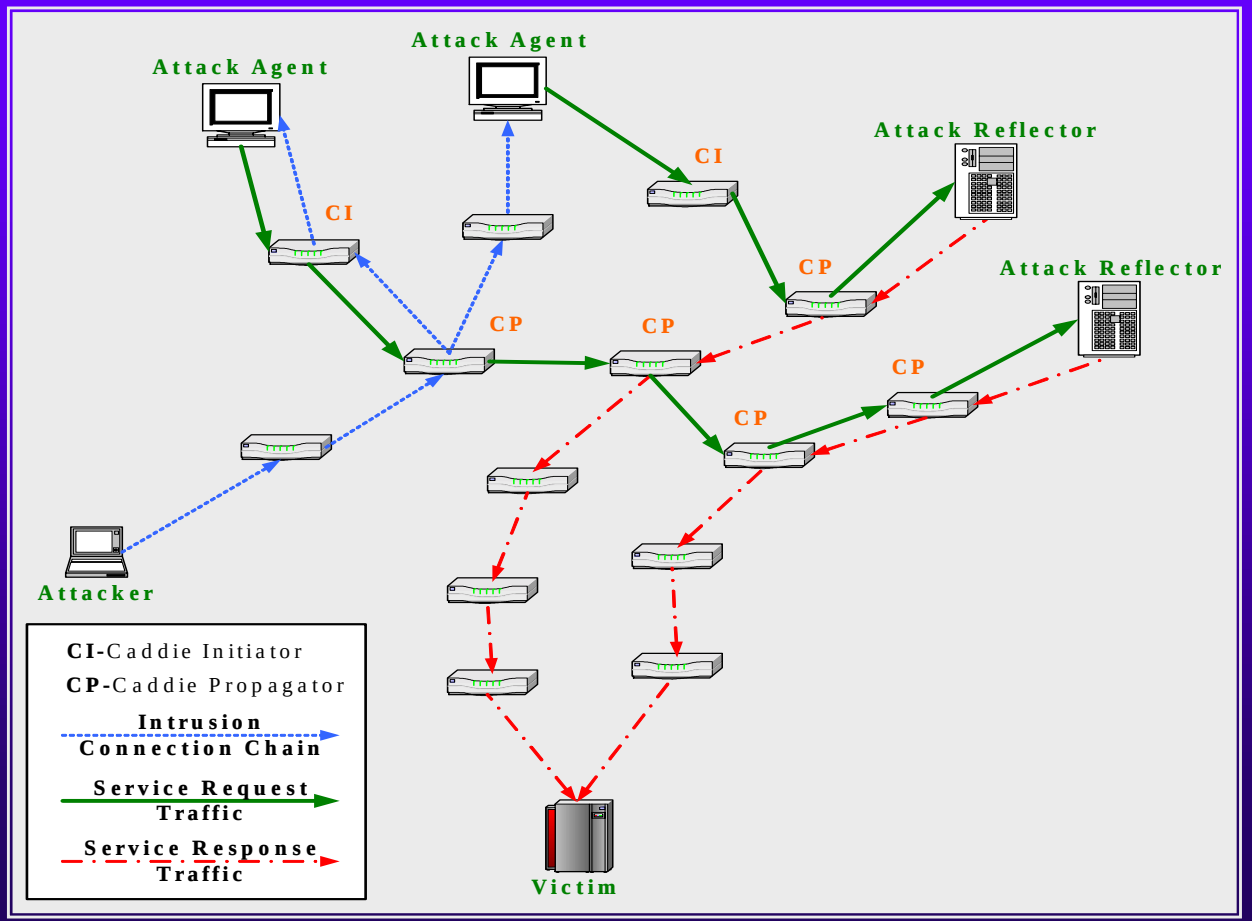
IP Traceback

- IP Traceback for Direct DDoS



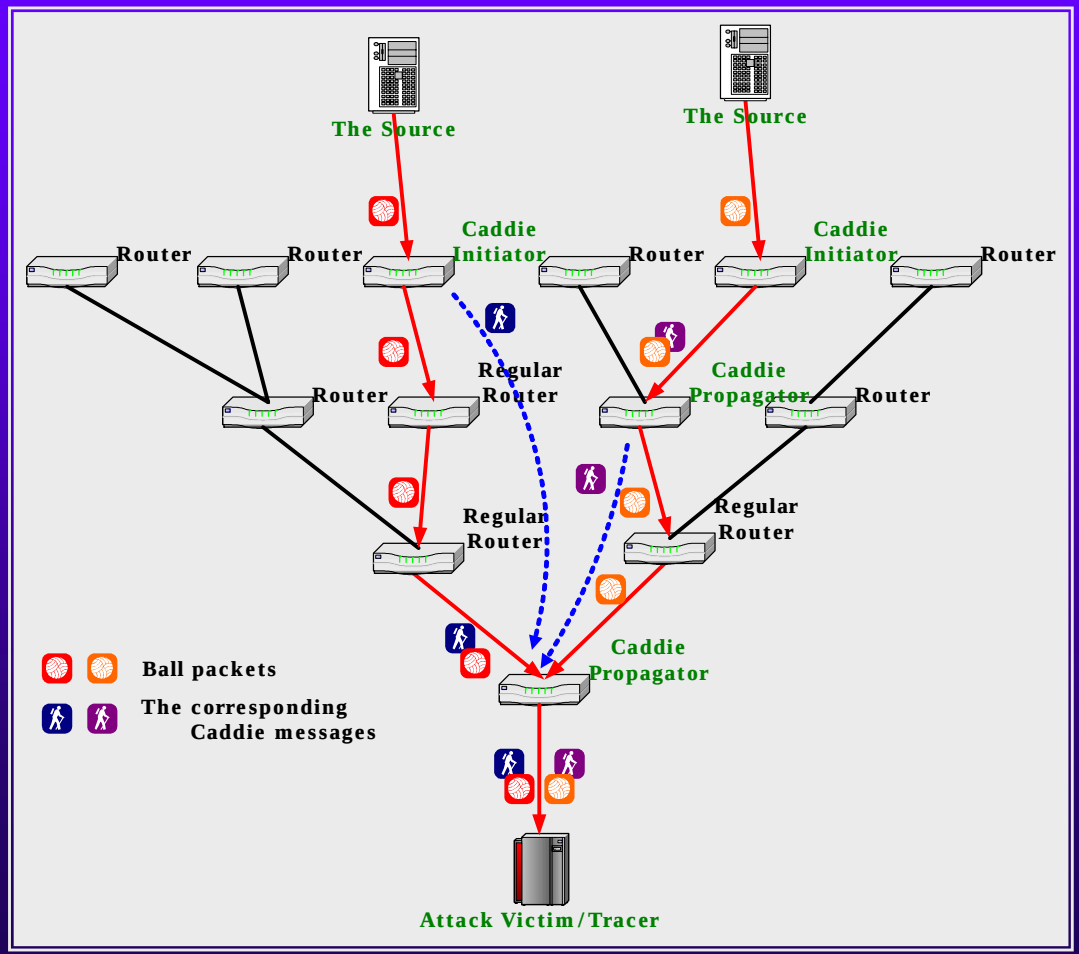
IP Traceback (Cont.)

- IP Traceback for Reflective DDoS



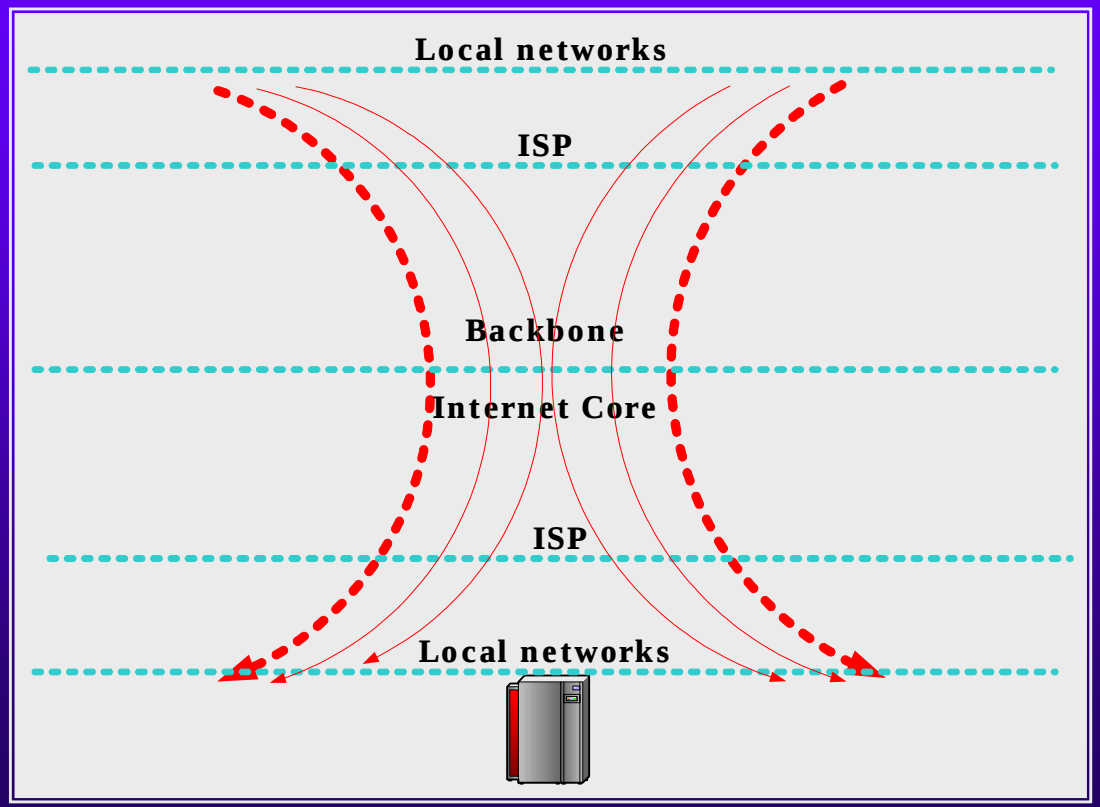
Evaluations

- Incremental Deployment
- Scalability



Evaluations (Cont.)

- Workload Distribution



Evaluations (Cont.)

- Security
  - HMACs
- Robustness
  - False positives
- Political Issues
  - ISPs' cooperation
  - Privacy

Evaluations (Cont.)

- Bandwidth Overhead
  - Number of attack packets required
  - Number of ICMP messages generated
- Storage Overhead
  - In the network
  - At the victim
- Computational Overhead
  - In the network
  - At the victim

Conclusion

- Effective
- Secure
- DoS-Resistant

Q&A

- Thank You Very Much