Distributed Denial of Service (DDoS): Attacks and Defenses

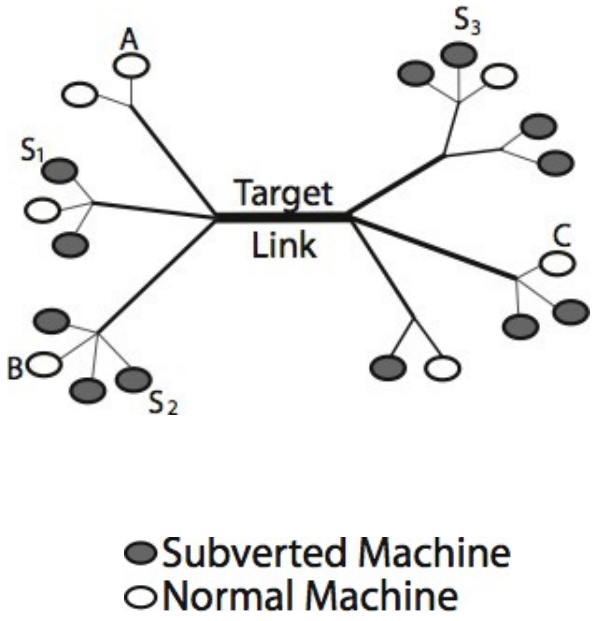
I. Pustogarov

The Coremelt attack (ESORICS'09)

- Source:
  - https://sparrow.ece.cmu.edu/group/pub/studer_esorics09.pdf
- Attacks the core network
  - Target links but not a specific server
- Use only "wanted" traffic
  - Botnets send/receive traffic among the bots
  - All legitimate connections
  - $O(N^2)$ connections between N bots

The Coremelt attack – steps

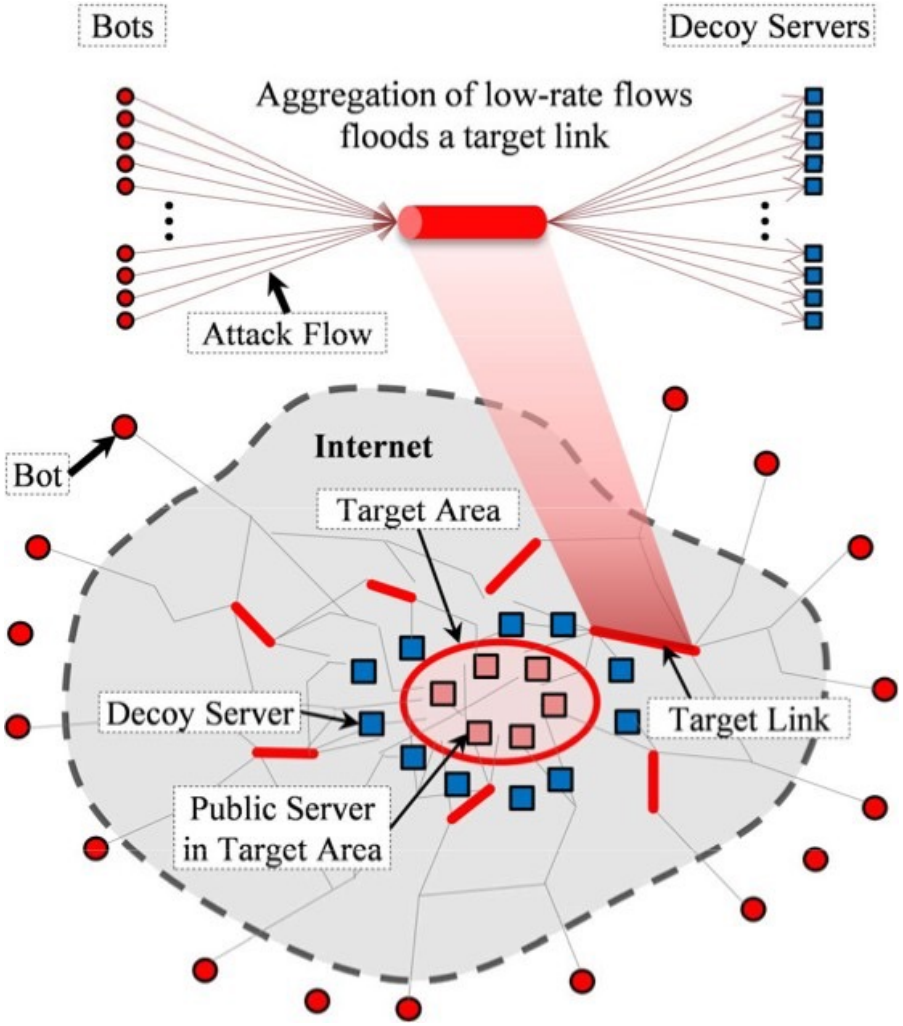
1. Select a link in the network as the target link
2. Identify what pairs of subverted machines can generate traffic that traverse the target link
3. Send traffic between the pairs identified in step 2 to overload the target link



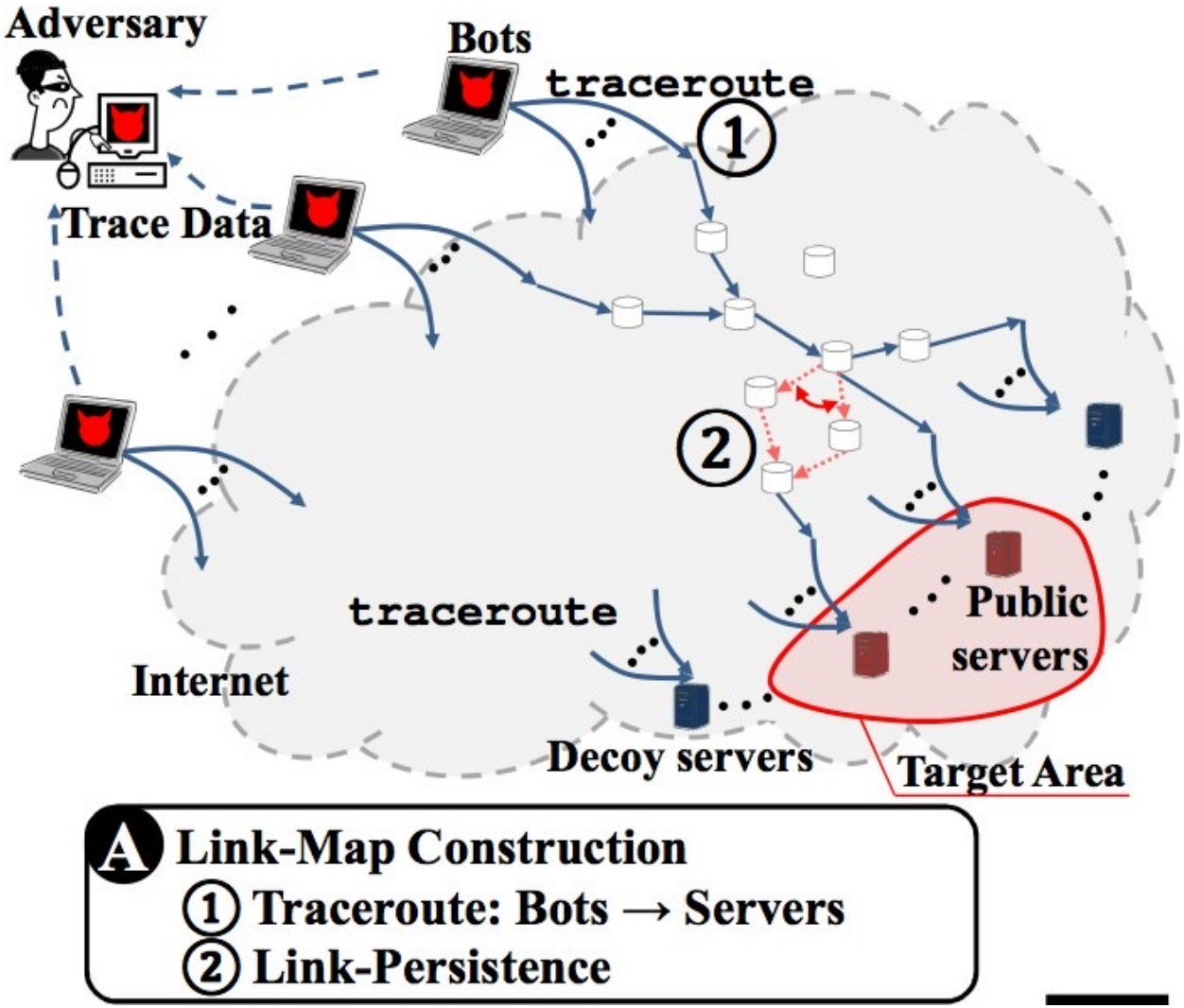
The Crossfire attack (Oakland'13)

- Source:
  - http://www.ieee-security.org/TC/SP2013/papers/4977a127.pdf
- Attack critical links of a target area
  - Target: an enterprise, city, state, small country)
- Uses public servers as decoys
- Low-intensity flows

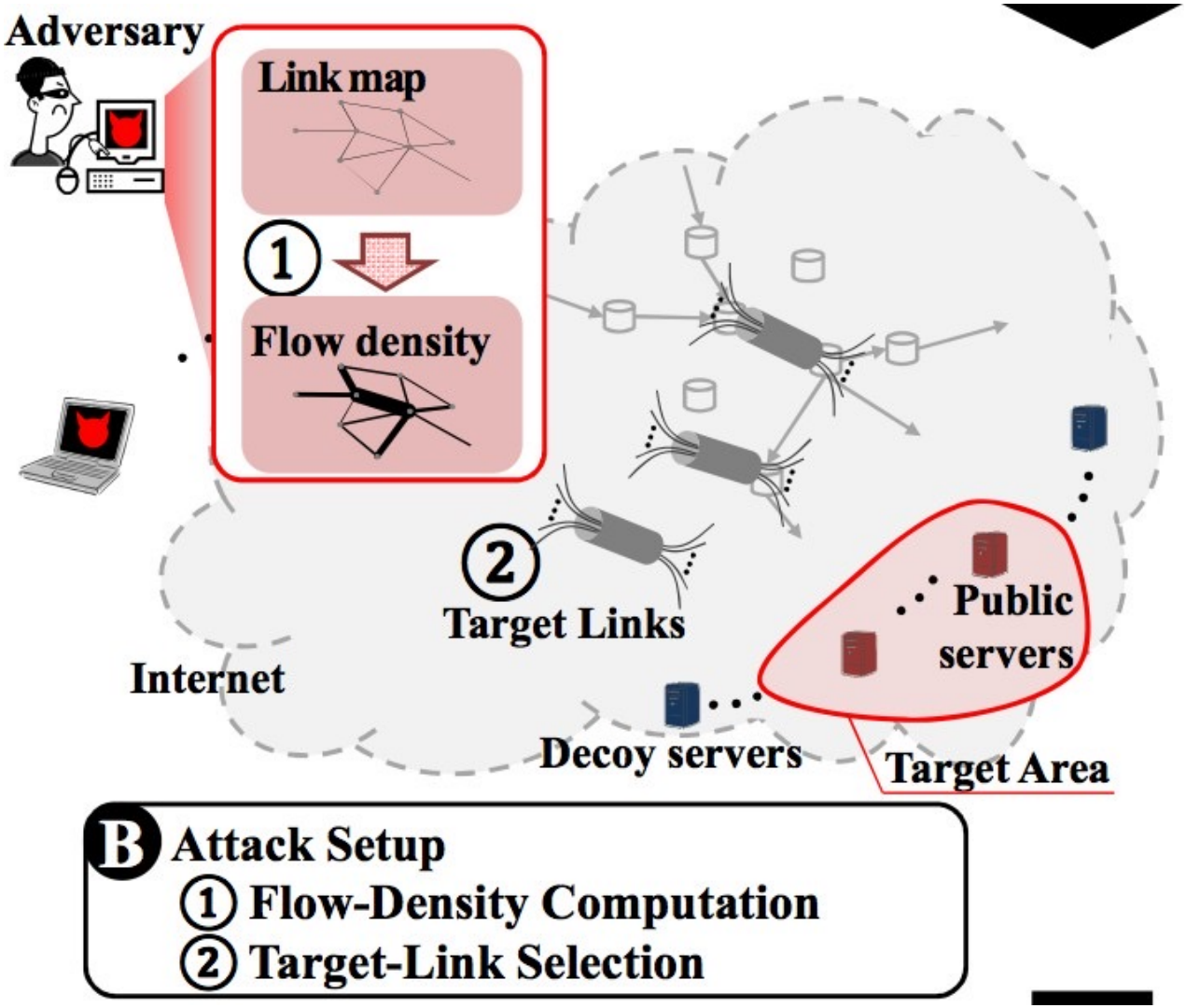
The Crossfire attack – overview



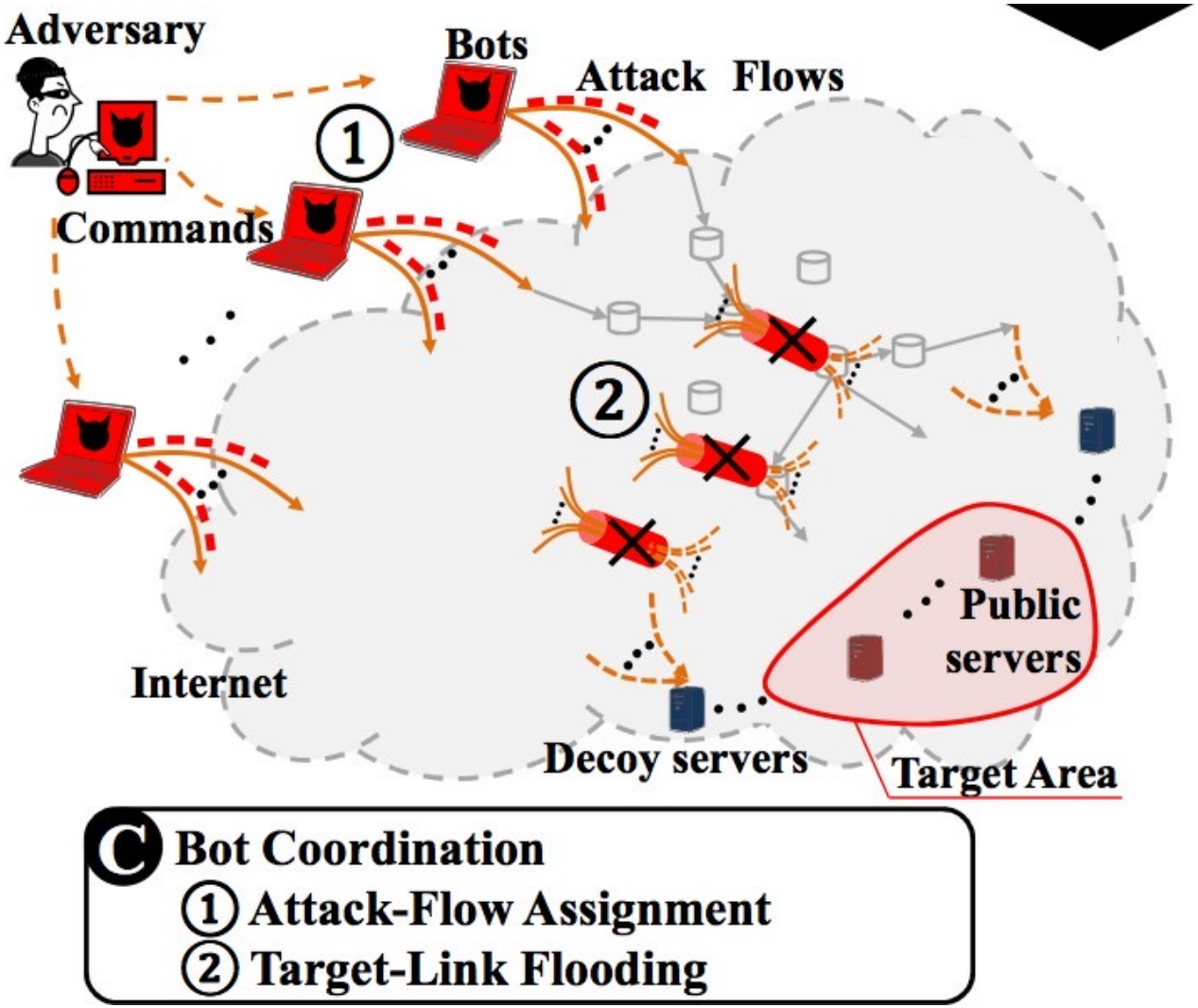
Step A: Link-map construction



Step B: Attack setup



Step C: Bot coordination



Important characteristics

- Undetectability at the target area
- Attack-flow indistinguishability
  - Different sets of (source-destination) IP addresses as seen by routers – difficult to trigger traffic aggregation-based mechanisms
- Persistence
  - Attackers can easily change bots and decoy servers
- Flexibility in selecting target area

The Spamhaus Attack
(March 18-22, 2013)

The Spamhaus attack

- Sources used:
  - CloudFlare: http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet
  - Ed Felten's blog: https://freedom-to-tinker.com/blog/felten/security-lessons-from-the-big-ddos-attacks/

- Possibly the largest DDoS attack so far in terms of attack traffic
  - Up to: 300Gbps
  - Degraded a lot of un-targeted services (in certain regions)
  - Tier-1 traffic congestion in Europe

Target(s) & attacker (s)

- Targets:
  - The Spamhaus Project website: http://www.spamhaus.org
    - Spamhaus track & publish anti-spam black lists
    - Email providers use Spamhaus service
  - CloudFlare (which was hosting Spamhaus.org)
    - Content delivery network (CDN) provider
  - "Peers" of CloudFlare

- Attackers:
  - Stophaus: group of "bulletproof spam and malware hosters"
  - Mainly: CyberBunker (Dutch ISP, hosted ThePirateBay & Wikileaks)
    - Another side of the attack: http://cyberbunker.com/web/spamhaus.php

Attack details

- Spamhaus moved to a CDN (CloudFlare) as a response to the initial attack (10Gbps or so)
- It's difficult to DDoS a CDN
- Attack CloudFlare's network peers (Tier2 ISPs)
  - The second-last network that connects a CloudFlare customer

- Method used:
  - DNS amplification (100 times!)
    - Source: PCs from a botnet
    - Destination: Spamhaus / CloudFlare peers