Trusted Networks Initiative to Combat DDoS Attacks

University of Amsterdam
System & Network Engineering
Research Project 1

Jeroen van Kessel
Alexandros Stavroulakis
Research Question

Is the "Trusted Networks Initiative" a feasible additional solution in protecting hosts and networks from large and/or long lasting DDoS attacks?
Problem Description

• The **size** of DDoS attacks keeps increasing
• Mitigation **costs** are also increasing
• No short term answer to this growing threat
Size of largest reported DDoS attacks

Source: Arbor Networks Worldwide Infrastructure Security Report, 2014
Top 10 countries of origin Q1 2014

Source: Incapsula Top 10 DDoS Attack Trends of 2014
DDoS Types & Mitigation Solutions

• **Attack types**
  • Volumetric Attacks
  • Application Layer Attacks

• **Mitigation Solutions**
  • Layer 3/4
  • Layer 7
DDoS Layer 7 Mitigation Solution
DDoS Layer 3/4 Mitigation Solution
Disadvantages

• Legitimate traffic discarded along with attack traffic
• Up to 30 minutes activation time is too long
• Privacy issues when serving https:// websites
• High cost
• The industry is always one step behind the attackers
Trusted Networks Initiative Concept

- A temporary last resort solution for DDoS attacks
- Dutch, internationally oriented initiative
- In combination with other Mitigation Solutions
- Trusted Routing to provide a secure interconnection for Trusted Networks
- Temporarily separate traffic from Trusted and Untrusted Networks
Trusted Networks Initiative Concept

- Responsibility for **proper Networking**
  - Advertise only **valid prefixes**
  - **Ingress Filtering** (address spoofing)
- **24/7 Collaboration** between participants
- **Forensic Investigation** on DDoS Attacks
Participants
Normal Routing, no DDoS Attack
Transit Networks

&

Internet Exchange Points (IXP)
Under DDoS Attack
How to mitigate a large DDoS Attack?
Trusted Routing

• Scenarios
  • On emergency Activation
  • Always On
Technical Analysis

- Uses already existent infrastructure and technology
- Traffic segregation via AS Numbers and IP ranges through BGP-4 routers
- Implementation of Anti-Spoofing with BCP 38
Conclusions

• DDoS attacks’ severity increases
• Trusted Networks Initiative is a feasible additional solution
• Critical services available to end-users even under attack
• Strong future marketing point
However

- Participants need to reach a consensus on its purpose
- Policies need to be finalized and timeframes to be specified
- Mobile Carriers as Trusted Networks
Thanks for your attention!

Jeroen van Kessel
Alexandros Stavroulakis