Blockchain-based Architecture for Collaborative DDoS Advertisement

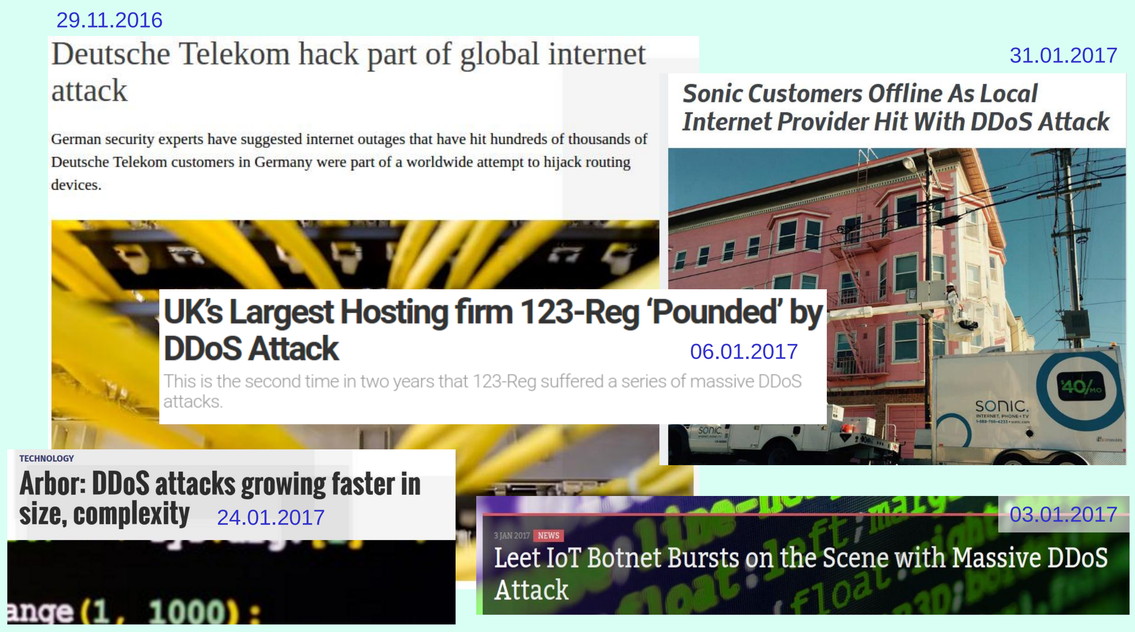
Department of Informatics Communication Systems Group

Peer-to-Peer Systems Engineering Lab (PS)

DDoS Attacks: Introduction and Challenges

Motivation

- DDoS attacks are getting **bigger**, more **frequent** and **sophisticated**
- **Unsecure IoT devices** have been used to launch massive DDoS attacks
- Layer 7 attacks are **hard to detect** and require understanding of underlying application

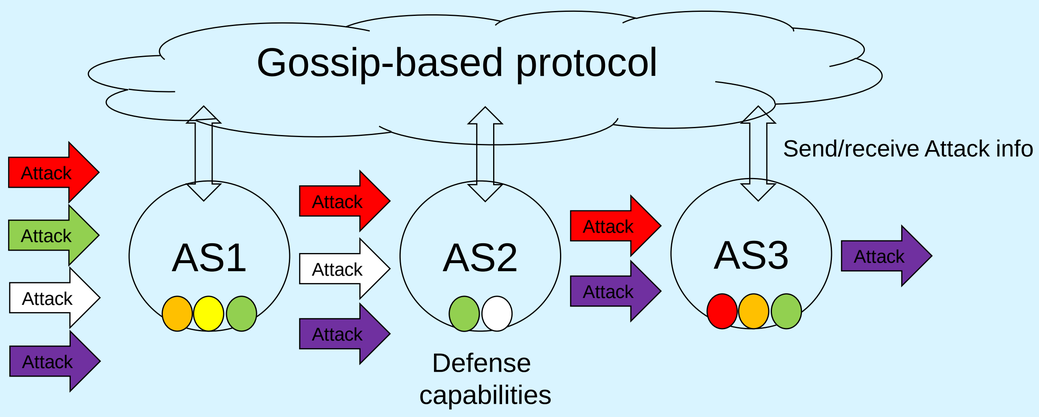


Attacks

- DDoS attack on **Deutsche Telekom** using IoT devices infected with the Mirai botnet.
- Launched in the end of December 2016, the **Leet Botnet achieved 650 Gbps of traffic**.
- DNS Reflection attacks, in which an **attacker can send 1 Gbps request and 100 Gbps** are delivered to the victim

Collaborative Approach

Gossip-based Protocols



Benefits

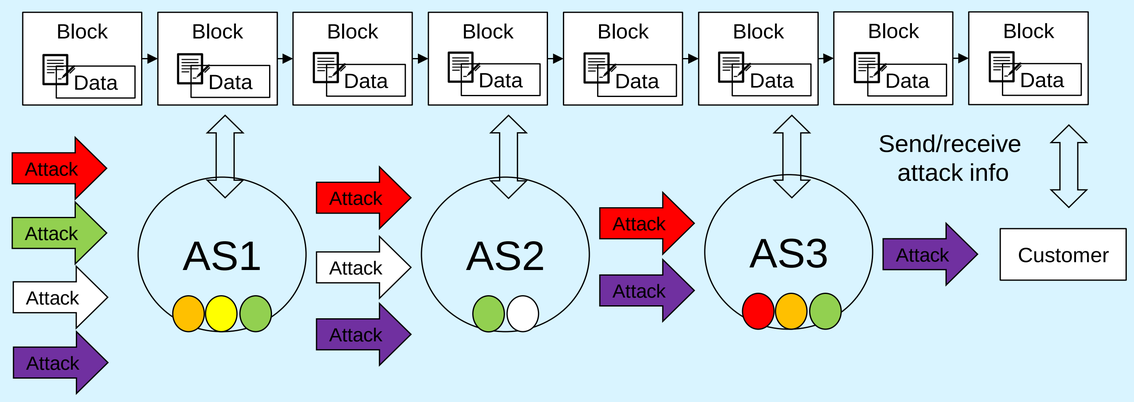
- Allows to **combine** defense capabilities of different ASes
- **Reduce the burden** of detection/mitigation in a single domain
- **Block malicious traffic near the source**

Related Work

Work	Protocol
DOTS 2017 (IETF)	DOTS protocol
Steinberger et al. 2016 (NOMS)	FLEX-based protocol
Sahay et al. 2015 (NDSS)	East/west bound protocols for SDN
Giotis et al. 2016 (NOMS)	East/west bound protocols for SDN
CoFence 2016 (CNSM)	Not declared

Blockchain-based Collaborative Approach

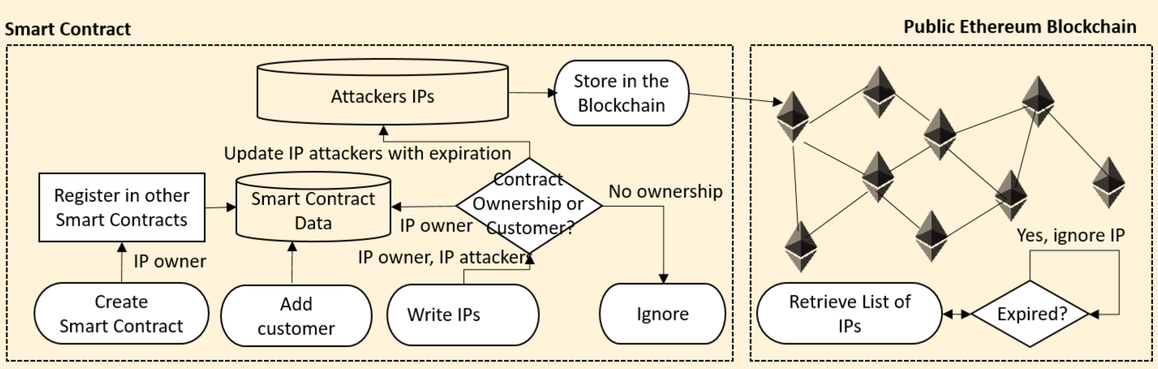
Blockchain-based Approach



Advantages

- **Public** and already **available** technology
- Can be deployed as an **additional security mechanism** without modifying existing mechanisms
- Appliances to read and write to the blockchain are **simple** to **develop** and **integrate**

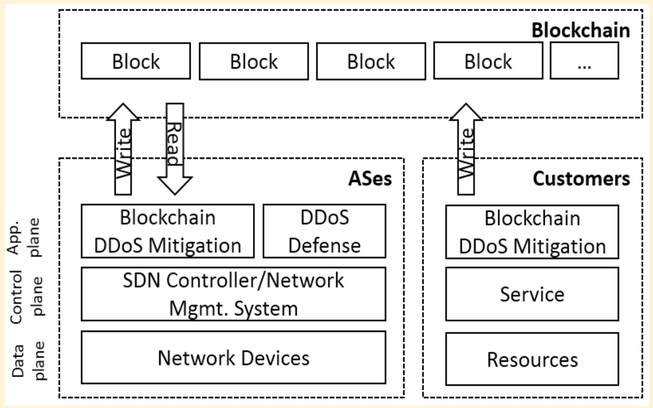
Smart Contracts



Solidity-based Smart Contract

- AS or customers **create contracts**; customers need to be **certified** to report addresses
- Smart contracts use a **registry-type entry**
- **Smart contract** data can use an URL to point to a list of addresses or a bloom filter

Preliminary Architecture



The blockchain-based approach is **simple** and **efficient to** advertise black or whitelisted IP addresses **across multiple** network domains

Ethereum Blockchain

- Blocks are mined every **14 seconds**
- **ASes** and verified **customers** can report/retrieve IP addresses
- **Black and whitelisted IP** addresses are supported
- **Low complexity** to integrate
- Existing security mechanisms and policies **do not need to be modified**

University of Zurich[UZH]

TECHNISCHE UNIVERSITÄT DARMSTADT

Find out more by visiting the CSG homepage:
http://www.csg.uzh.ch

Bruno Rodrigues *rodrigues@ifi.uzh.ch*
Dr. Thomas Bocek *bocek@ifi.uzh.ch*
Prof. Dr. David Hausheer *hausheer@ps.tu-darmstadt.de*
Andri Lareida *lareida@ifi.uzh.ch*
Sina Rafati *rafati@ifi.uzh.ch*
Prof. Dr. Burkhard Stiller *stiller@ifi.uzh.ch*

ifi